NTFS Security Management Suite

NTFS Security Management Suite 2014
Copyright © 2014 Vyapin Software Systems Private Limited. All Rights Reserved.
Email: support@vyapin.com Web: www.vyapin.com

Last Updated: June 2015

Copyright © 2014 **Vyapin Software Systems Private Limited**. All rights reserved.

This document is being furnished by Vyapin Software Systems Private Ltd for information purposes only to licensed users of the NTFS Security Management Suite 2014 software product and is furnished on an "AS IS" basis, that is, without any warranties, whatsoever, express or implied. External Data Connector is a trademark of Vyapin Software Systems Private Ltd. Information in this document is subject to change without notice and does not represent any commitment on the part of Vyapin Software Systems Private Ltd. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software except as specifically allowed in that license. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to the way of: photocopying, recording, or information recording and retrieval systems, without the express written permission of Vyapin Software Systems Private Ltd.

Vyapin Software Systems Private Limited

Website: http://www.vyapin.com/
Sales Contact: sales@vyapin.com
Technical Support: support@vyapin.com

GENERAL INFORMATION 1

About NTFS Security Management Suite 2014 ..... **2**

System Requirements **4**

How to purchase? **5**

How to activate the software? **6**

Technical support **8**

CONFIGURATION SETTINGS 9

Database Settings **10**

Configure Computer Enumeration **13**

Configuring Domain Credentials **14**

Add a domain **17**

Edit a domain **19**

Delete a domain **21**

Add domains from forest **23**

Configure SMTP Server **26**

User Connection Profiles **27**

Module Listing **30**

NTFS SECURITY AUDITOR 31

Built-in Reports **32**
About Built-in Reports 33
How to view Built-in Permissions Reports? 34
How to view Built-in Reports for Shares and Resources? 88

Shares, Folders and Files **92**
How to view Shares, Folders and Files information? 93

DAC Reports **97**
About DAC Reports 98
How to view the effective DAC permissions for the specified accounts? 99
How to view the effective DAC permissions for Accounts having permissions on specific folders? 107

How to view Central Access Policies and policy permissions? 113
How to check the shared folders and subfolders affected by DAC policies? 117

Security Viewer 123
How to view the permissions for shares and local drives? 124
How to enumerate shared folders/files? 132

Power Search 137
About Power Search 138
How to view Power Search Permissions (DACL) Reports? 139
How to view Power Search Exceptions (DACL) Reports? 149
How to view Power Search Auditing (SACL) Reports? 159
How to manage Power Search? 169

Compare ACLs 171
About Compare ACLs 172
How to Compare ACLs of folders? 173
How to Compare ACLs of a folder with exported ACL data of another folder? 177

Security Vulnerabilities 182
How to view Security Vulnerabilities Reports? 183

Power Export 227
About Power Export 228
Scheduled Tasks Manager 229
Schedule Shares, Folders and Files Reports 233
Schedule Built-in Reports 242

NTFS SECURITY MANAGER 338

Grant Permissions 339
About Grant Permissions 340
How to Grant Permissions for selected Shares? 347
How to reuse the Grant Permissions template? 358

Revoke Permissions 360
About Revoke Permissions 361
How to revoke permissions from the selected shares permissions list? 376
How to reuse the Revoke Permissions template? 393

Modify Permissions 395
How to view the share permissions? 396
How to Grant Permissions for selected Shares? 402
How to add new accounts to the folder/file permissions list? 412
How to replace an account with another account in the shared folder/file permissions list? 419
How to remove the selected account from the shared folder/file permissions list? 426
How to allow inheritance from the parent to current folder/file permissions? 428
How to block inheritance from the parent to the current folder/file permissions? 430
How to modify an account Basic permissions? 433

How to modify an account Advanced permissions? 436

Copy Permissions 439
About Copy Permissions....440
How to Copy Permissions from one share to another share(s)? 447
How to reuse the Copy Permissions template? 461

Copy Account Permissions 463
How to copy account permissions in the selected shared folder(s)/file(s) permissions list? 464

Dynamic Access Control 472
How to Apply Central Access Policy on selected Shares? 473
How to Revoke Central Access Policy from the selected Shares?....482

Power Search 495
About Power Search....496
How to view Power Search Permissions (DACL) Reports? 497
How to manage Power Search? 506

Change History 508
About Change History 509
How to view Permissions Change History? 510
How to view Central Access Policies Change History? 514

ADDITIONAL FEATURES 516

How to customize fields? 517

How to Apply Filter? 518

How to Refresh data? 520

How to Export data? 521

How to E-mail data? 523

How to find data in a report? 527

SCAN PROFILES MANAGER 529

About Scan Profiles (Computers) 530

How to create Scan Profiles (Computers)? 531

How to manage Scan Profiles (Computers)? 536

How to apply Scan Profiles (Computers) in NTFS Security Auditor Module? 538

How to apply Scan Profiles (Computers) in NTFS Security Manager Module? 540

About Scan Profiles (Users/Groups) **543**

How to create Scan Profiles (Users/Groups)? **544**

How to manage Scan Profiles (Users/Groups)? **549**

How to apply Scan Profiles (Users/Groups) in NTFS Security Auditor Module? **551**

How to apply Scan Profiles (Users/Groups) in NTFS Security Manager Module? **556**

About Scan Profiles (Shares) **559**

How to create Scan Profiles (Shares)? **560**

How to manage Scan Profiles (Shares)? **565**

How to apply Scan Profiles (Shares) in NTFS Security Auditor Module? **567**

How to apply Scan Profiles (Shares) in NTFS Security Manager Module? **572**

REFERENCES 574

Frequently Asked Questions **575**

Troubleshooting **576**

How to uninstall NTFS Security Management Suite 2014? **577**

General Information

About NTFS Security Management Suite 2014

System Requirements

How to purchase?

How to activate the software?

Technical support

About NTFS Security Management Suite 2014

Vyapin NTFS Security Management Suite 2014 is a powerful solution for auditing and managing NTFS security across your entire Windows network. The management suite consists of two modules – the NTFS Security Auditor module and the NTFS Security Manager module.

About NTFS Security Auditor Module

NTFS Security Auditor Module provides a powerful reporting solution for auditing NTFS security across your entire Windows network. NTFS Security Auditor module provides answers to important questions about the security and health of File systems in your servers and workstations.

- Who has access to what in your Files, Folders and Shares? Is there any unauthorized access?
- What type of access has been granted? Who can Read, Modify and Delete confidential Files and Folders?
- Do deleted or unknown users have access to files and folders?
- Who have been given special/explicit permissions on folders? Do the normal rules such as "inheritance of permissions by folders from parent" apply or have they been broken or subverted?
- Who have unauthorized access to confidential files and folders indirectly because of nested group membership?
- Are people sharing folders from their workstations? Are there Shares in workstations that need further security scrutiny?
- What type of permissions and conditions have been configured for each the Central Access Rules (CAR) in Central Access Policy (CAP) over the domain controller (Windows Server 2012)?
- Who have access limited permissions by Dynamic Access Control (DAC)/Central Access Policy (CAP) on Which folder?
- Which shared folders and subfolders (in Windows Server 2012) have been affected/not affected by the Central Access Policy?

With Vyapin's NTFS Security Auditor Module you can perform a complete security scan of Shares, Folders and Files present in your network. You can perform an automated inventory of permissions on Folders and Files at regular intervals and keep a constant watch on the health of your NTFS security. You can also view the effective DAC (Dynamic Access control) permissions in Windows Server 2012. Our solution provides a variety of audit reports that are simple, elegant and highly customizable for System

Administrators, IT infrastructure Managers and Systems Audit personnel to use and act on. There are several powerful, ready-to-use reports that assist in both Management reporting and Compliance reporting requirements such as SOX and HIPAA. Vyapin's NTFS Security Auditor serves your needs of administrative tasks as well as complex data preparation tasks for assisting in compliance.

About NTFS Security Manager Module

NTFS Security Manager module provides a powerful Management tool for managing NTFS Security across your entire Windows network. NTFS Security Manager module helps to manage the security of File systems in your servers and workstations.

- Grant permissions in bulk for multiple Accounts to your Files, Folders and Shares.
- Replace existing permissions with new permissions.
- Remove selected Accounts with all its permissions from the Files, Folders and Shares permissions list.
- Copy permissions from one File, Folder and Share to bulk of Files, Folders and Shares permissions list.
- Remove permissions from explicitly assigned Account permissions.
- Allow or Block inheritance from the parent Share, Folder into the current File, Folder and Share.
- View and Modify each Account permissions on Shares, Folders and Files.
- Replace an account with another account in the shared folder/file permissions list.
- Apply Central Access Policy on shared folder(s)/file(s).
- Revoke Central Access Policy from the shared folder(s)/file(s).

Vyapin's NTFS Security Management Suite 2014 has been architected using the latest Microsoft .NET technology, bringing you the best-in-breed NTFS reporting and management solution for your entire Windows Network. The software is highly optimized for performance (using native Windows API calls wherever appropriate), resulting in fast data collection of permissions from Shares, Folders and Files. You can create data subsets for your network using powerful scan options and meaningfully segment your entire network for data collection, reporting and managing.

System Requirements

For the computer running NTFS Security Management Suite 2014

Disk space & Memory	512 MB RAM and minimum of 30 MB of free disk space
Operating System	Windows 8.1 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2003 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 with .NET Framework 4.0 or higher with the latest service packs.
Database	Microsoft SQL Server 2012 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2008 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2005 (Enterprise / Standard / Developer / Express edition) running in local / remote computer with latest Service Pack.
Software	MDAC v2.5/2.6/2.8

For the computers reported and managed by NTFS Security Management Suite 2014

Windows 8.1 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2012 R2 / Windows Server 2012 / Windows Server 2008 / Windows Server 2008 R2 / Windows 2003.

How to purchase?

You can purchase NTFS Security Management Suite 2014 online from our website http://www.vyapin.com/.

Please contact our Sales department at sales@vyapin.com for sales and price related queries.

How to activate the software?

Once you purchase the software online or through any one of our resellers, you will receive a sale notification through e-mail from our sales department. We will send you an e-mail with the necessary instructions to activate the software.

In case you do not receive an e-mail from our sales team after you purchase the software, please send the following information to our sales department at sales@vyapin.com with the sales order number:

- **Company Name**: End-user Company Name
- **Location**: City & Country for the Company Name given above

Please allow 12 to 24 hours from the time of purchase for our sales department to process your orders.

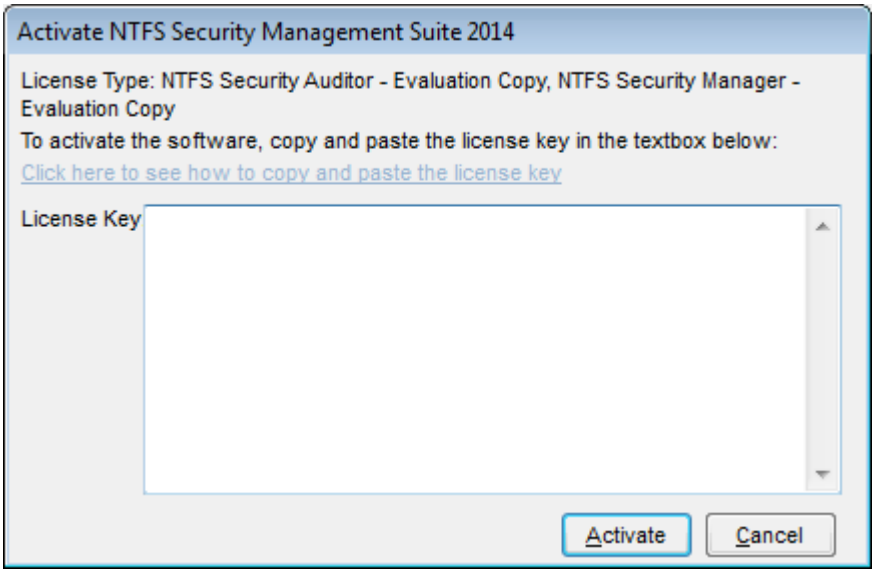

Activate NTFS Security Management Suite 2014
License Type: NTFS Security Auditor - Evaluation Copy, NTFS Security Manager - Evaluation Copy
To activate the software, copy and paste the license key in the textbox below:
Click here to see how to copy and paste the license key
License Key
Activate
Cancel

Image 1 – Activate screen

Perform the following steps to activate the software:

1. Download evaluation/trial copy of software from the respective product page available in our website at http://www.vyapin.com/
2. Install the software on the desired computer.
3. You will receive a license key through e-mail as soon as the purchase process is complete.
4. Click 'Activate' in Application Menu -> About -> Activate menu to see the Activate dialog (as shown in Image 1).
5. Copy the license key sent to you through email and paste it in the 'License Key' textbox. For help on how to copy the license key, click 'Click here to see how to copy and paste the license key' link in the Activate dialog (as shown in Image 2).

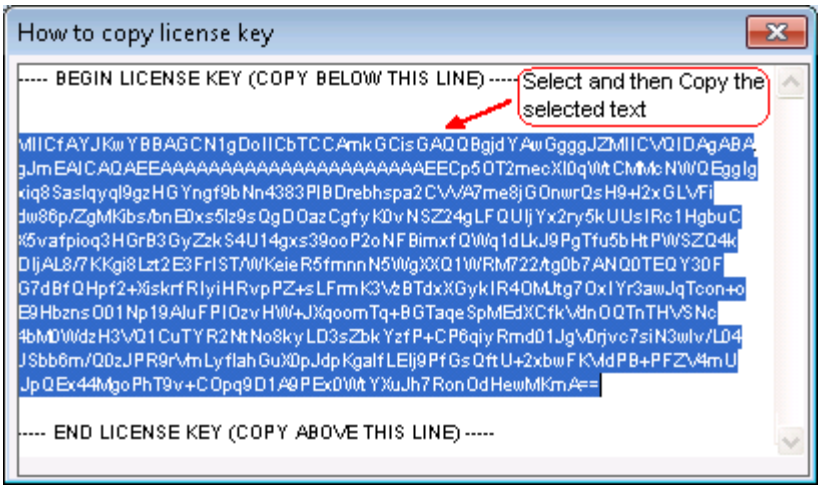


Image 2 – How to copy license key screen

Technical support

NTFS Security Management Suite 2014 Frequently Asked Questions (FAQ) section is available online at our website http://www.vyapin.com.

Please direct all technical support questions to support@vyapin.com. Include the following information to expedite a response:

a. Include the version of the product you are using.
b. If the problem is associated with installation, include the steps that led to the problem.
c. If the problem is associated with usage, please state the series of steps you performed.
d. Include the version of the OS, info about any service packs or hot-fixes and local language of the OS installed.
e. Attach the Error Log File available in the common application data path of NTFS Security Management Suite 2014 (e.g., <Application Data> \NTFS Security Management Suite 2014\NTFSSecurityManagementSuite2014ErrorLog.Log).

Note:

<Application Data> is the common area where NTFS Security Management Suite 2014 settings will be stored in the computer running NTFS Security Management Suite 2014.The <Application Data Folder> can be found from the Help -> About screen. The default path of <Application Data Folder> is as follows: The path will be as follows:

a. Windows XP, Windows 2003 - C:\Documents and Settings\All Users\Documents
b. Windows Server 2008, Windows Server 2012, Windows Vista, Windows 7, Windows 8 - C:\Users\Public\Documents

Configuration Settings

Database Settings

Computer Enumeration

Configuring Domain Credentials

Add a domain

Edit a domain

Delete a domain

Add domains from forest

Configure SMTP serves

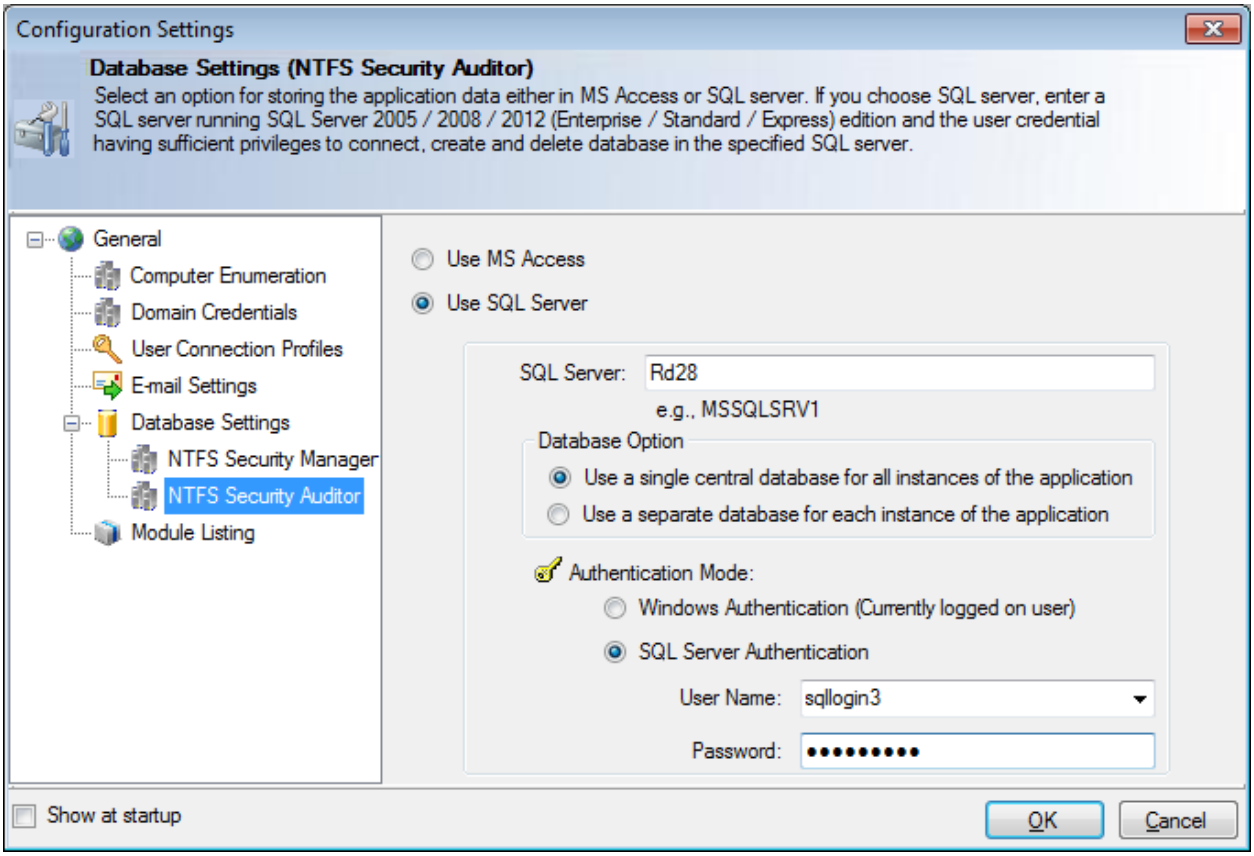
User Connection Profiles

Module Listing

Database Settings

NTFS Security Management Suite 2014 may be configured to use either MS-Access MDB or SQL Server database for its data storage to generate reports. If you choose SQL server NTFS Security Auditor module requires an SQL Server running SQL Server 2005 / 2008 / 2012 (Enterprise / Standard / Express editions) to connect and create a new application database. NTFS Security Management Suite 2014 will connect to the specified SQL Server based on authentication mode and user credentials to manage its own application database.

You can access the Database settings by clicking **Configuration -> Configuration Settings** menu in the NTFS Security Management Suite 2014 main application window and choose Database settings, as shown below.


Configuration Settings
Database Settings (NTFS Security Auditor)
Select an option for storing the application data either in MS Access or SQL server. If you choose SQL server, enter a SQL server running SQL Server 2005 / 2008 / 2012 (Enterprise / Standard / Express) edition and the user credential having sufficient privileges to connect, create and delete database in the specified SQL server.
General
Computer Enumeration
Domain Credentials
User Connection Profiles
E-mail Settings
Database Settings
NTFS Security Manager
NTFS Security Auditor
Module Listing
Use MS Access
Use SQL Server
SQL Server: Rd28
e.g., MSSQLSRV1
Database Option
Use a single central database for all instances of the application
Use a separate database for each instance of the application
Authentication Mode:
Windows Authentication (Currently logged on user)
SQL Server Authentication
User Name: sqllogin3
Password: ••••••••••
Show at startup
OK
Cancel

User Authentication

To connect to SQL Server, NTFS Security Management Suite 2014 uses the relevant user accounts based on the authentication mode as listed below:

A. Windows Authentication:

In this method, NTFS Security Management Suite 2014 uses the currently logged on user account while running reports

B. SQL Authentication:

In this method, NTFS Security Management Suite 2014 uses the specified SQL user account and password while running reports. NTFS Security Management Suite 2014 module stores the SQL user name and password as a user profile in 'Stored User Names and Passwords' applet for its usage.

Read User Connection Profiles for more details.

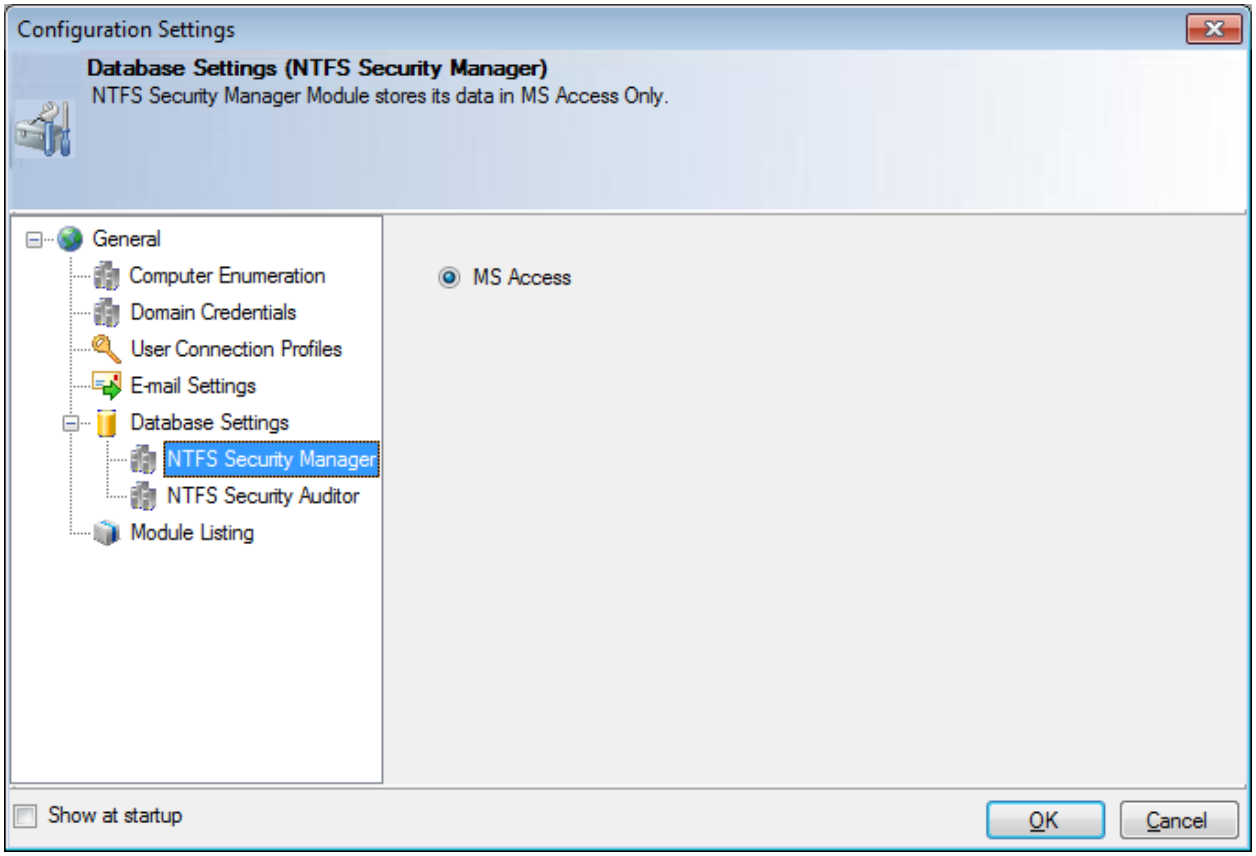
Note: NTFS Security Management Suite 2014 expects the user account to have sufficient privileges to create, add to and delete database in the SQL server.

Database creation

NTFS Security Management Suite 2014 creates databases in SQL Server based on the following database options (whichever is selected) as outlined below:

1. Use a single central database for all instances of the application
   - A new database will be created in the SQL server by the name NTFSSecurityManagementSuite2014. Inside the NTFSSecurityManagementSuite2014 database, separate tables will be created for each installation of NTFS Security Management Suite 2014. The table names will be prefixed with the computer name that is running NTFS Security Management Suite 2014 application. Thus, each installation of NTFS Security Management Suite 2014 will deploy its own tables based on the computer where NTFS Security Management Suite 2014 is installed. For example, if you install the software on 3 different computers, single database with 3 different tables will be created inside the single database and each installed application will generate reports separately independent of each other.
   - NTFSSecurityManagementSuite2014tmpSchduleInfo database will be created in the SQL server for scheduled tasks.
2. Use a separate database for each instance of the application
   - NTFS Security Management Suite 2014 module creates a single application database in the default data storage location used by the SQL Server during application launch. NTFS Security Management Suite 2014 uses the following naming convention: NTFSSecurityManagementSuite2014-<COMPUTERNAME>, where COMPUTERNAME is the name of the computer running NTFS Security Management Suite 2014.
   - NTFSSecurityManagementSuite2014tmpSchduleInfo<COMPUTERNAME> database will be created in the SQL server for scheduled tasks.
   - For example, if the computer running the NTFS Security Management Suite 2014 is ‘CLIENT01’, NTFS Security Management Suite 2014 creates 'NTFSSecurityManagementSuite2014-CLIENT01' with data ('NTFSSecurityManagementSuite2014-CLIENT01.mdf') and log (''NTFSSecurityManagementSuite2014-CLIENT01_log.LDF') files stored in the default SQL data folder in the SQL server (for example, C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data).

NTFS Security Manager module stores its data in use MS-Access database.



Database cleanup

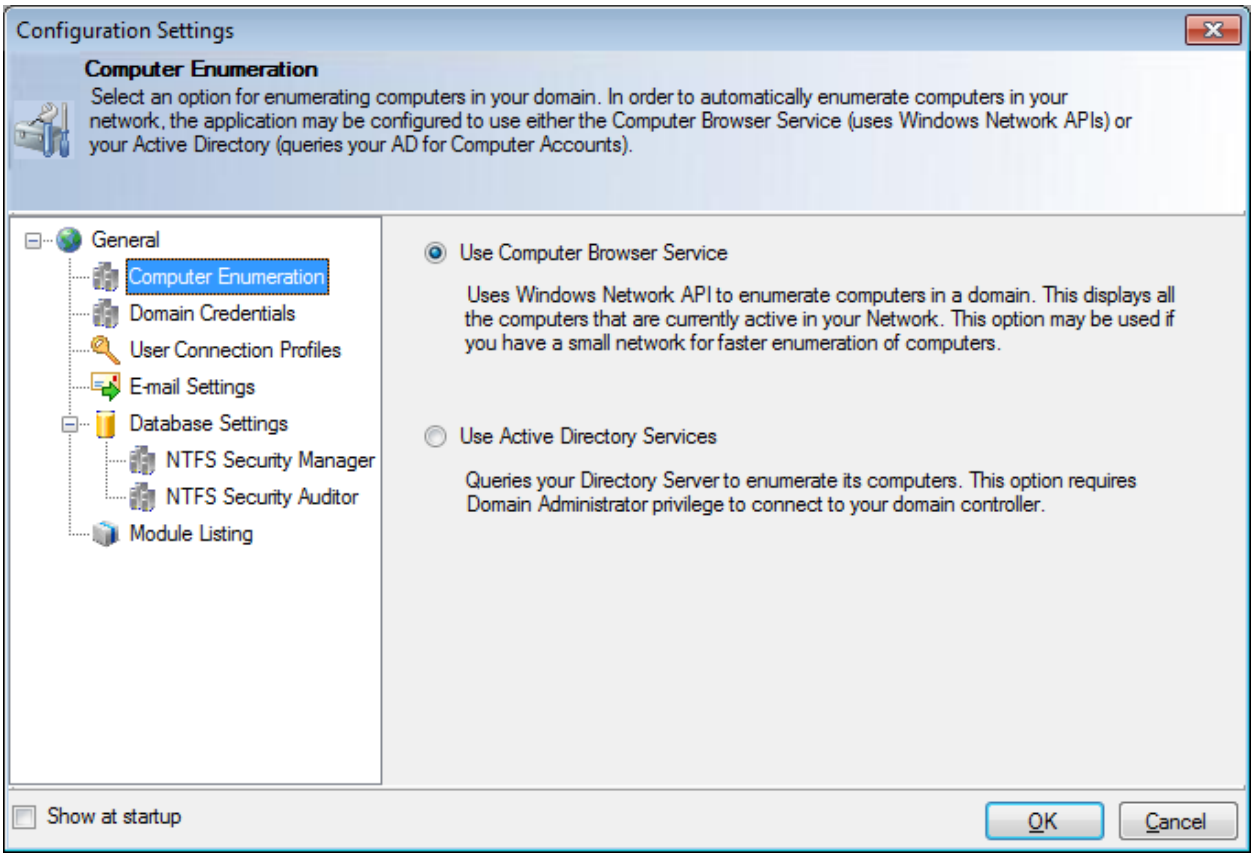
'NTFS Security Management Suite 2014' will delete the application database while uninstalling the 'NTFS Security Management Suite 2014' application from the computer.

Configure Computer Enumeration

For enumerating computers in your network automatically, NTFS Security Management Suite 2014 uses either Computer Browser Service or Active Directory Services. Select an option for enumerating computers in your domain as shown below. You may use the Browser service if you have a smaller network, as it may take time for the Browser service to respond to data requests on large networks. The advantage of a Browser service is that it lists only those computers that are currently active/alive on your network. You may use the Active Directory Services option if you have a large network and you need a quicker enumeration of computers in your domain. However, this option requires that the domain controller is contacted and queried. Therefore, the currently logged on user must have sufficient privileges to connect to a domain controller or you may specify alternate domain credentials for a domain controller (see configuring the Domain Credentials section in the wizard).

NOTE: If you use the Browser service, ensure that NETBIOS over TCP/IP is enabled in both the client and the computers that need to be reported on. The Browser service must also be running.

You can access the Computer Enumeration settings by clicking Configuration -> Configuration Settings in the NTFS Security Management Suite 2014 main application window and selecting "Computer Enumeration" node as shown below:

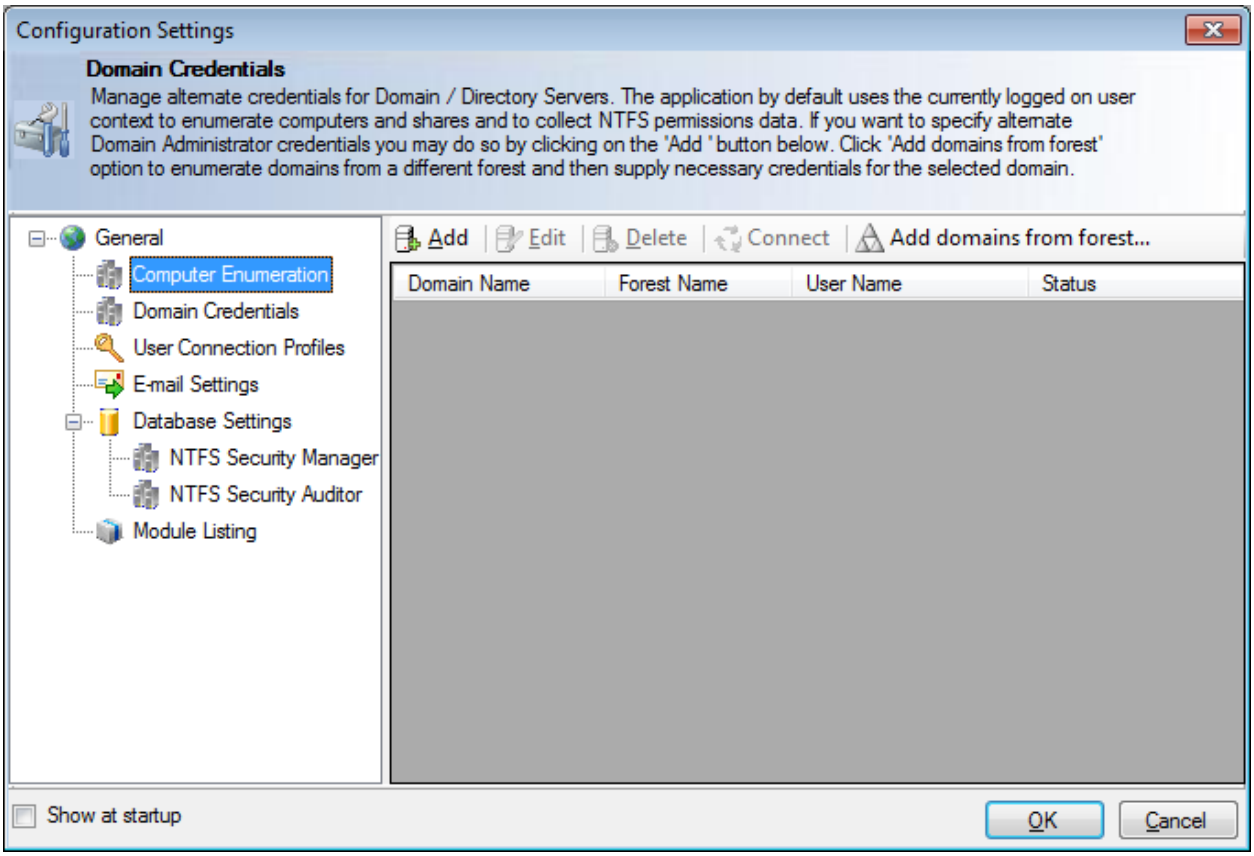

Configuration Settings
Computer Enumeration
Select an option for enumerating computers in your domain. In order to automatically enumerate computers in your network, the application may be configured to use either the Computer Browser Service (uses Windows Network APIs) or your Active Directory (queries your AD for Computer Accounts).
General
Computer Enumeration
Domain Credentials
User Connection Profiles
E-mail Settings
Database Settings
NTFS Security Manager
NTFS Security Auditor
Module Listing
Use Computer Browser Service
Uses Windows Network API to enumerate computers in a domain. This displays all the computers that are currently active in your Network. This option may be used if you have a small network for faster enumeration of computers.
Use Active Directory Services
Queries your Directory Server to enumerate its computers. This option requires Domain Administrator privilege to connect to your domain controller.
Show at startup
OK
Cancel

Configuring Domain Credentials

Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers and shares and to collect NTFS permissions data. If you want to specify alternate Domain Administrator credentials you may use this option.

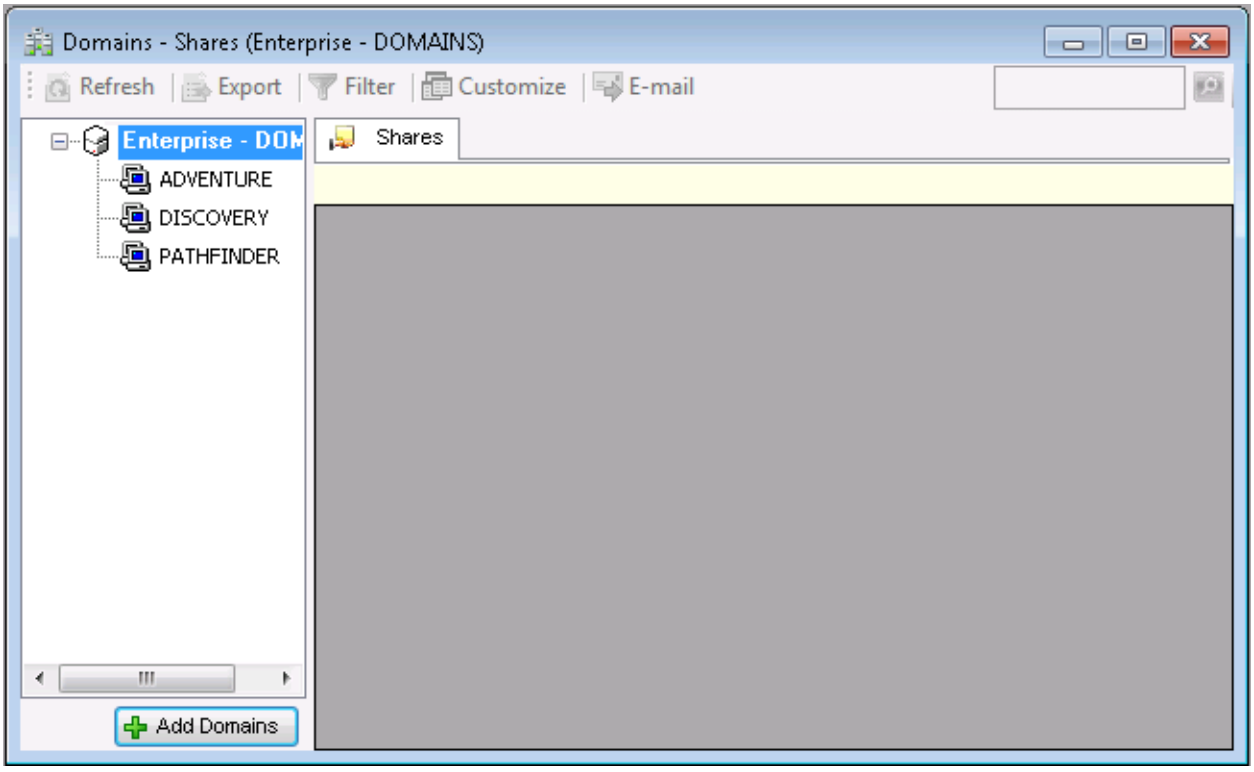
Configuring Domain Credentials

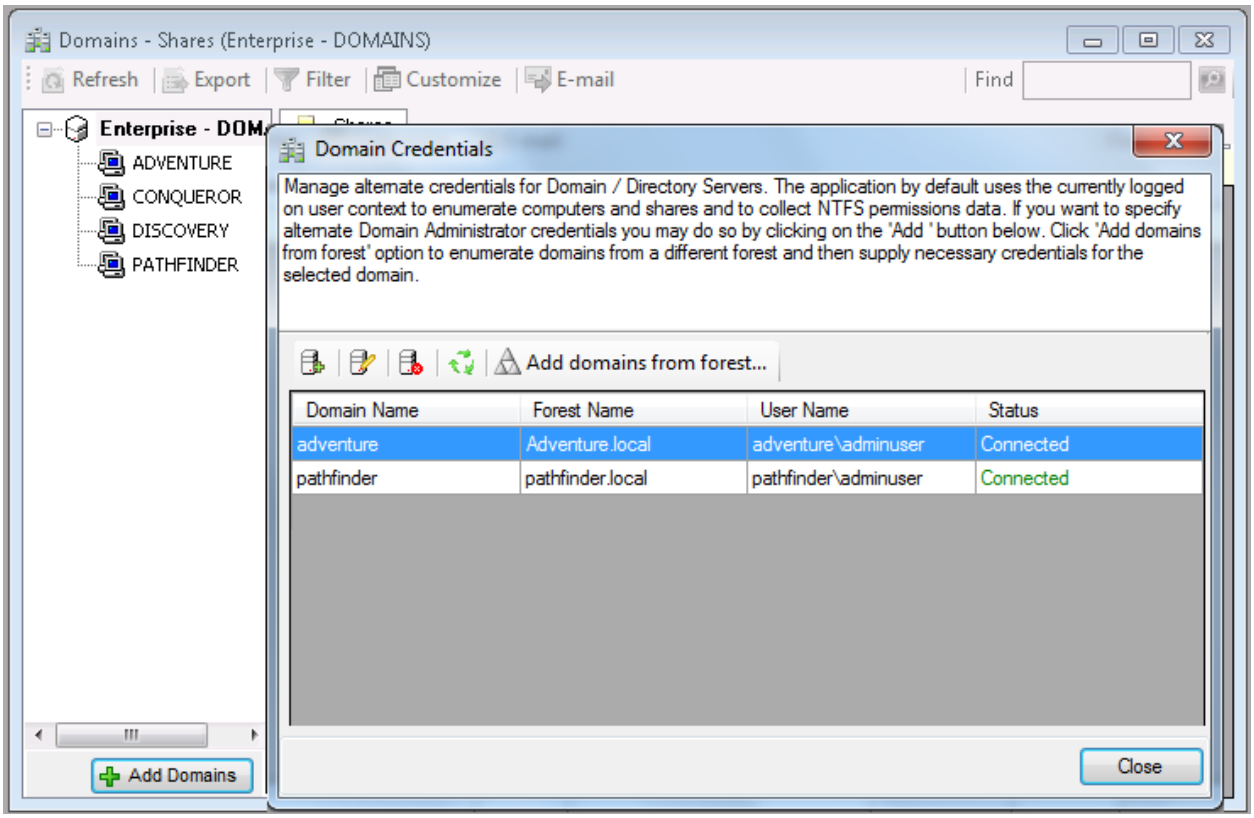
You can access the Domain Credentials settings by selecting the Domain Credentials option in the Configuration Settings window.


Configuration Settings
Domain Credentials
Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers and shares and to collect NTFS permissions data. If you want to specify alternate Domain Administrator credentials you may do so by clicking on the 'Add ' button below. Click 'Add domains from forest' option to enumerate domains from a different forest and then supply necessary credentials for the selected domain.
General
Computer Enumeration
Domain Credentials
User Connection Profiles
E-mail Settings
Database Settings
NTFS Security Manager
NTFS Security Auditor
Module Listing
Add
Edit
Delete
Connect
Add domains from forest...
Domain Name
Forest Name
User Name
Status
Show at startup
OK
Cancel

If you have chosen Active Directory Services under the Computer Enumeration settings, you can launch the NTFS Security Auditor Domain Credentials window within a report window by doing the following:

1. Select any one of the reports from the NTFS Security Management Suite 2014 main application window. For example Standard Reports -> Domains-Shares option.
2. The action will launch the Domains-Shares report window.
3. In the reports windows, at the bottom of the treeview click **Add Domains** button. This action will launch the "**Domain Credentials**" windows as shown below.


Domains - Shares (Enterprise - DOMAINS)
Refresh
Export
Filter
Customize
E-mail
Enterprise - DOM
ADVENTURE
DISCOVERY
PATHFINDER
Shares
Add Domains


Domains - Shares (Enterprise - DOMAINS)
Refresh
Export
Filter
Customize
E-mail
Find
Enterprise - DOM
ADVENTURE
CONQUEROR
DISCOVERY
PATHFINDER
Add Domains
Domain Credentials
Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers and shares and to collect NTFS permissions data. If you want to specify alternate Domain Administrator credentials you may do so by clicking on the 'Add ' button below. Click 'Add domains from forest' option to enumerate domains from a different forest and then supply necessary credentials for the selected domain.
Add domains from forest...
Domain Name
Forest Name
User Name
Status
adventure
Adventure.local
adventure\adminuser
Connected
pathfinder
pathfinder.local
pathfinder\adminuser
Connected
Close

The various operations that can be performed in the Domain Credentials screen are given below:

Operation	Description
Add	To Add a new domain to the list.
Edit	To Edit the properties of a domain in the list. Select a domain and click Edit button.
Delete	To Delete a domain from the list. Select a domain and click Delete button.
Connect	To connect to a domain in the list. Select a domain and click Connect button.

Add a domain

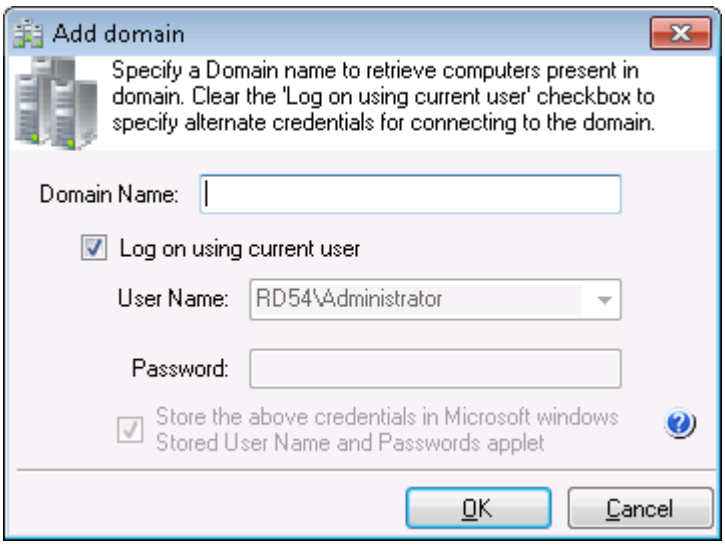
You may also add one single domain at a time to the list of domains in the credentials list by using Add Domain feature.

Add a domain to the list

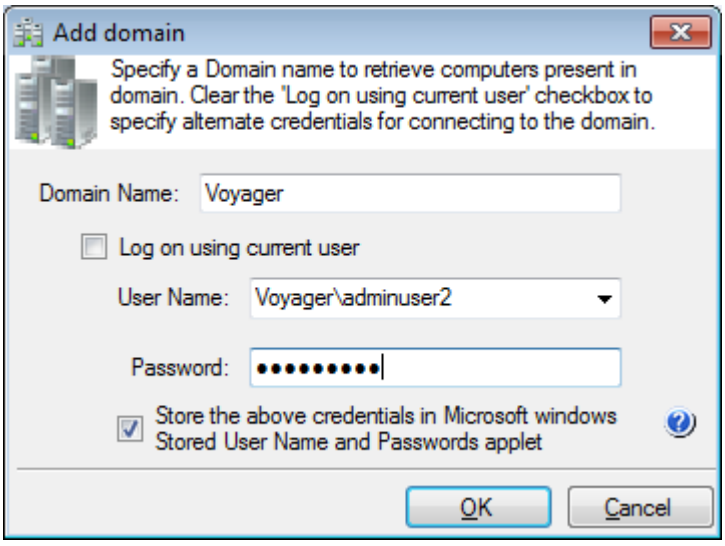
1. Launch Domain Credentials window.

2. In the Domain Credentials window, click Add button to add a domain to the list.

3. The New domain connection dialog will be displayed as shown below:


Add domain
Specify a Domain name to retrieve computers present in domain. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the domain.
Domain Name:
Log on using current user
User Name:
RD54\Administrator
Password:
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
OK
Cancel

Enter the name of a domain.


Add domain
Specify a Domain name to retrieve computers present in domain. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the domain.
Domain Name:
Voyager
Log on using current user
User Name:
Voyager\adminuser2
Password:
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
OK
Cancel

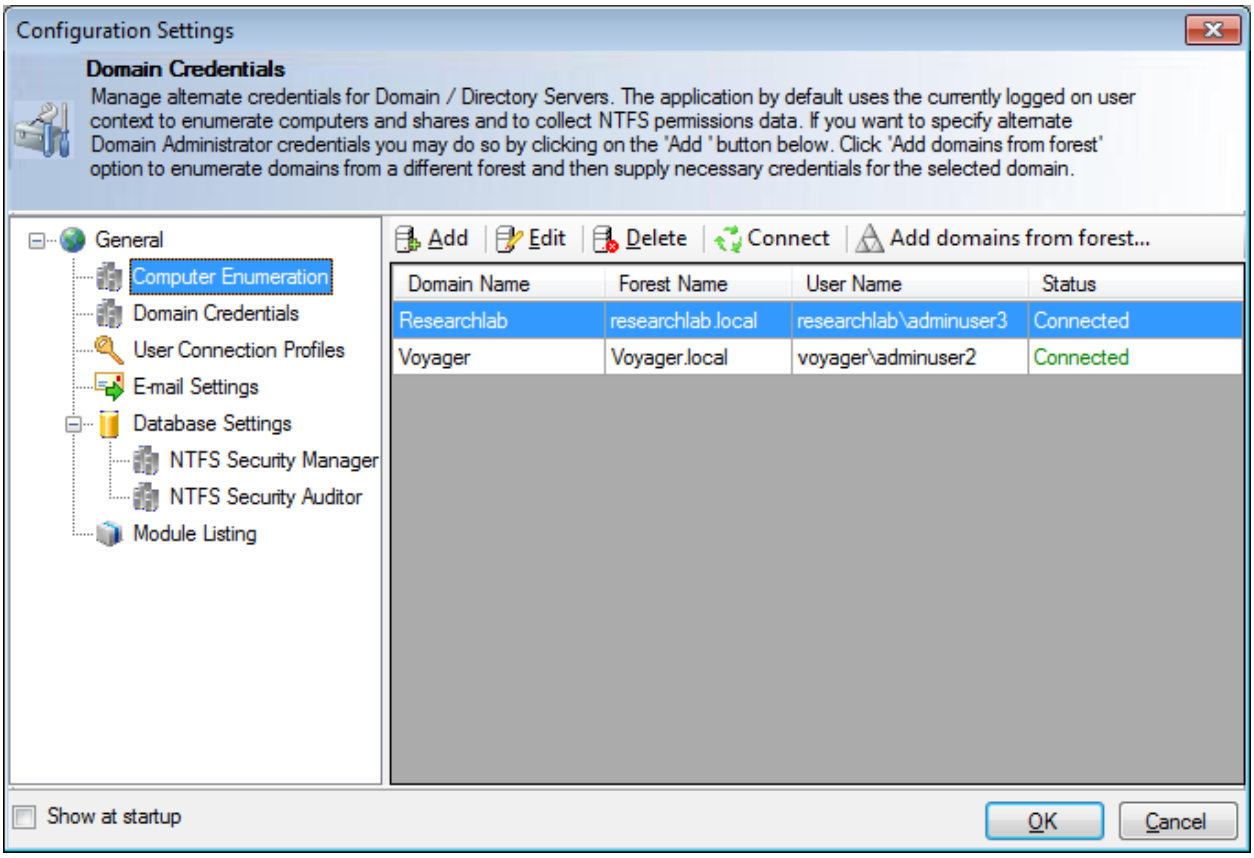
4. Specify user name and the corresponding password to connect to the specified domain.

Store the above user credential in **Microsoft Windows Stored User Names and Passwords applet** - NTFS Security Management Suite 2014 allows the user to enter different user credentials to connect to the domain. Uncheck the checkbox 'Log on using current user' if you like to connect to the domain using a different user context.

NTFS Security Management Suite 2014 will store the user credential to connect to domain in the Microsoft Windows Stored User Names and Passwords applet / Credential Manager for security reasons. The stored user profile is tied to the user context (currently logged on user account) in which the profile is created.

5. Click OK to add the domain to the Domain Credentials list.

6. NTFS Security Management Suite 2014 will connect to the domain with the newly provided connection parameters and add it to the list, upon successful connection to the domain.



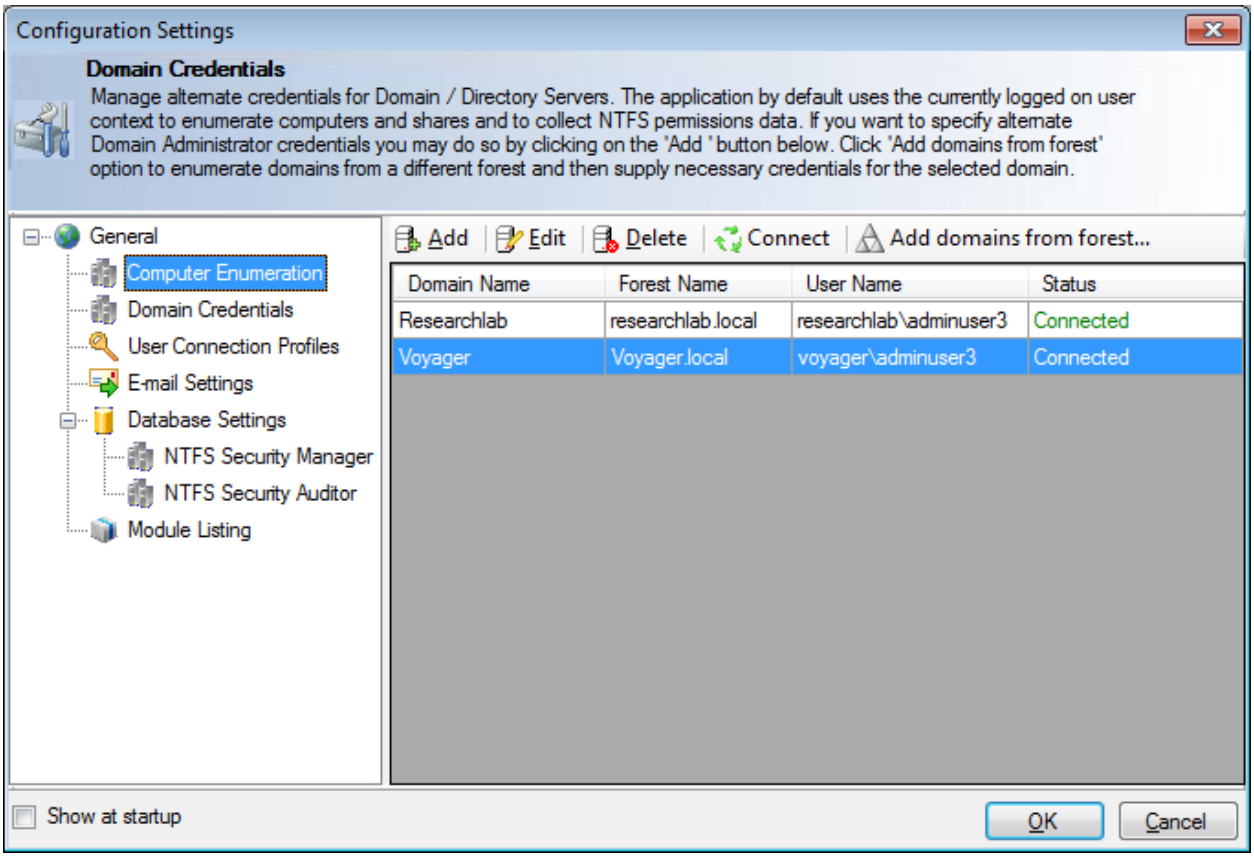
7. Click Cancel to abort the add process of the domain to the Domain Credentials list.

Edit a domain

To Edit a domain in the Domain Credentials, follow the steps given below:

1. Launch Domain Credentials window.

2. In the Domain Credentials window, select any row (domain), Click Edit button to Edit an existing domain in the list, as shown below:

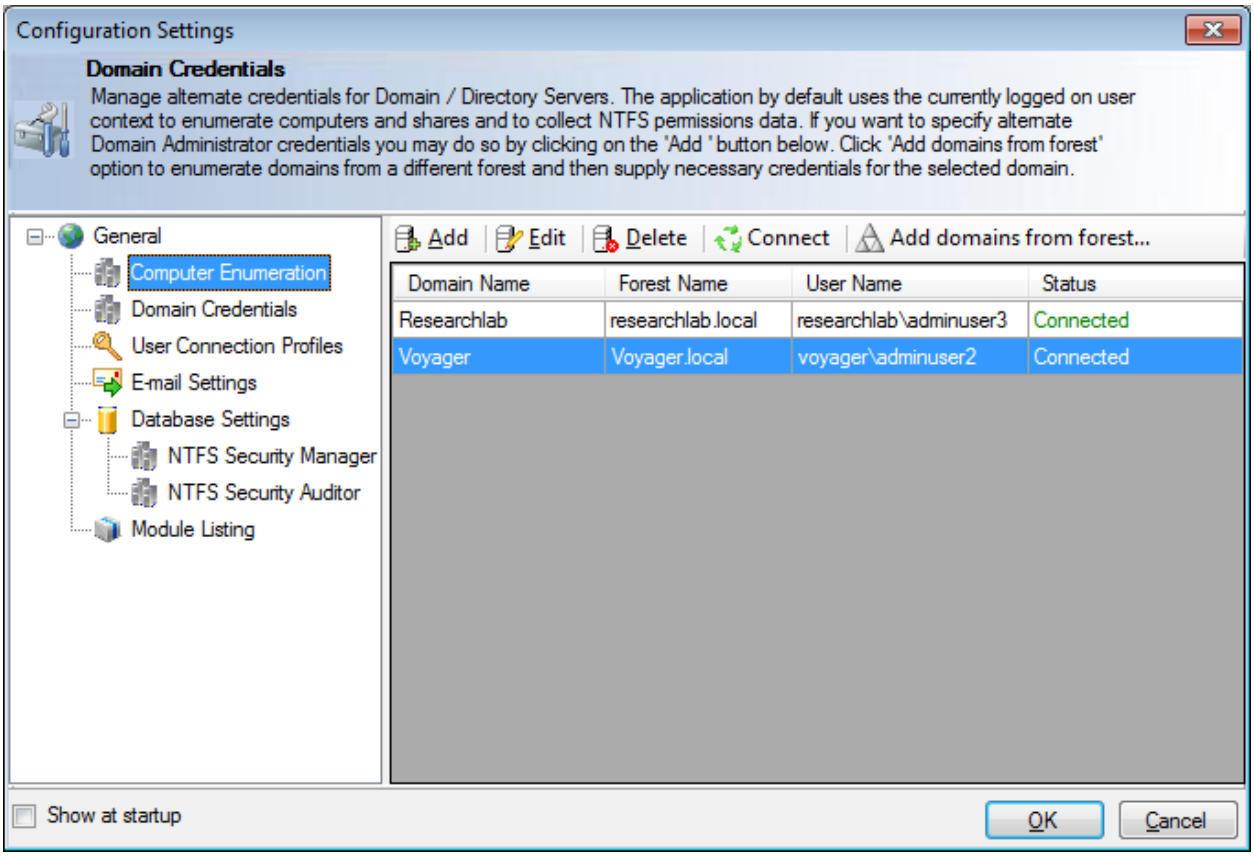


3. The domain name cannot be modified during the edit operation.

4. Specify user name and the corresponding password to connect to the specified domain.

5. Click OK to save and connect to the domain with the newly provided connection parameters and update the domain in the Domain Credentials list.

6. NTFS Security Management Suite 2014 will connect to the domain with the newly provided connection parameters and modify it in the list, upon successful connection to the domain.



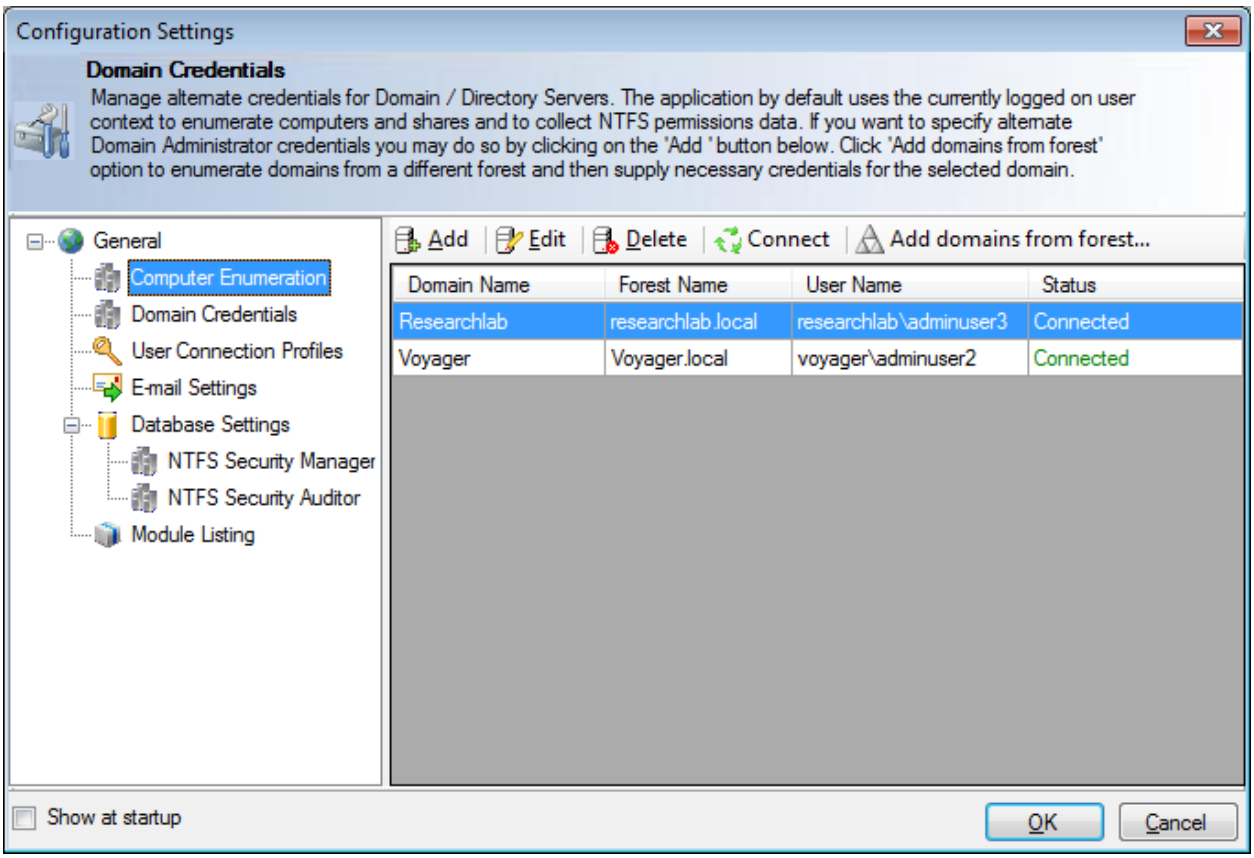
7. Click **Cancel** to retain the existing connection parameters of the domain in the Domain Credentials list.

Delete a domain

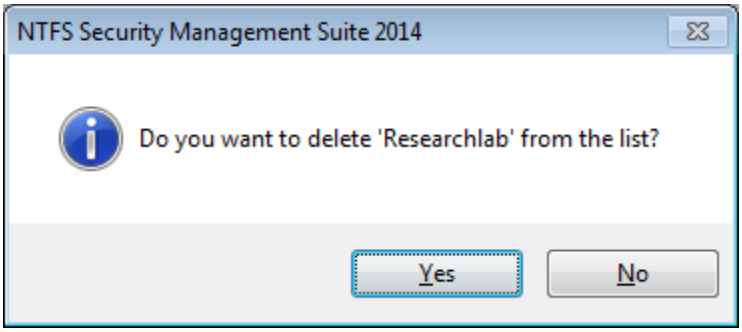
Perform the following steps to delete a domain:

1. Launch Domain Credentials window.

2. In the Domain Credentials window, select any row (domain), click Delete button to delete the forest from the Domain Enumeration Manager list.



3. An alert message asking for confirmation to delete the forest will be displayed as shown below:



4. Click Yes to delete the selected forest.

5. Click No to abort the delete process of the selected forest.

Add domains from forest

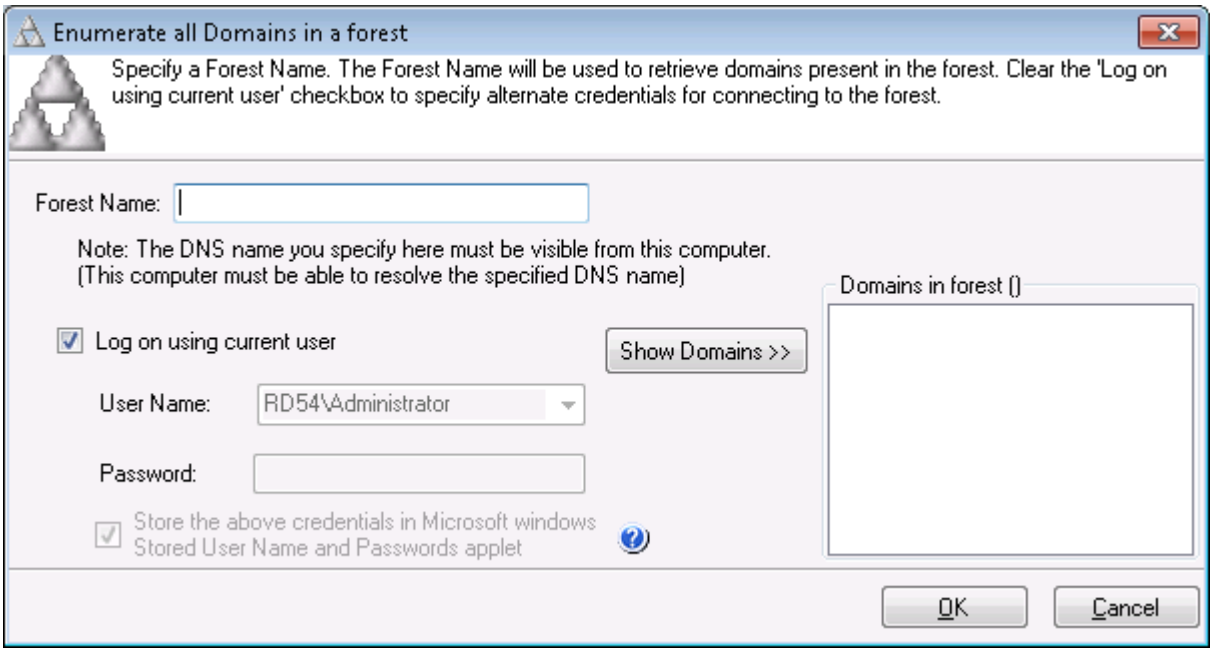
In order to connect to a different forest in your Active Directory and configure these domains for enumerating computers and generating reports on them, you may use the 'Add Domains from Forest' feature.

Add domains from forest to the list

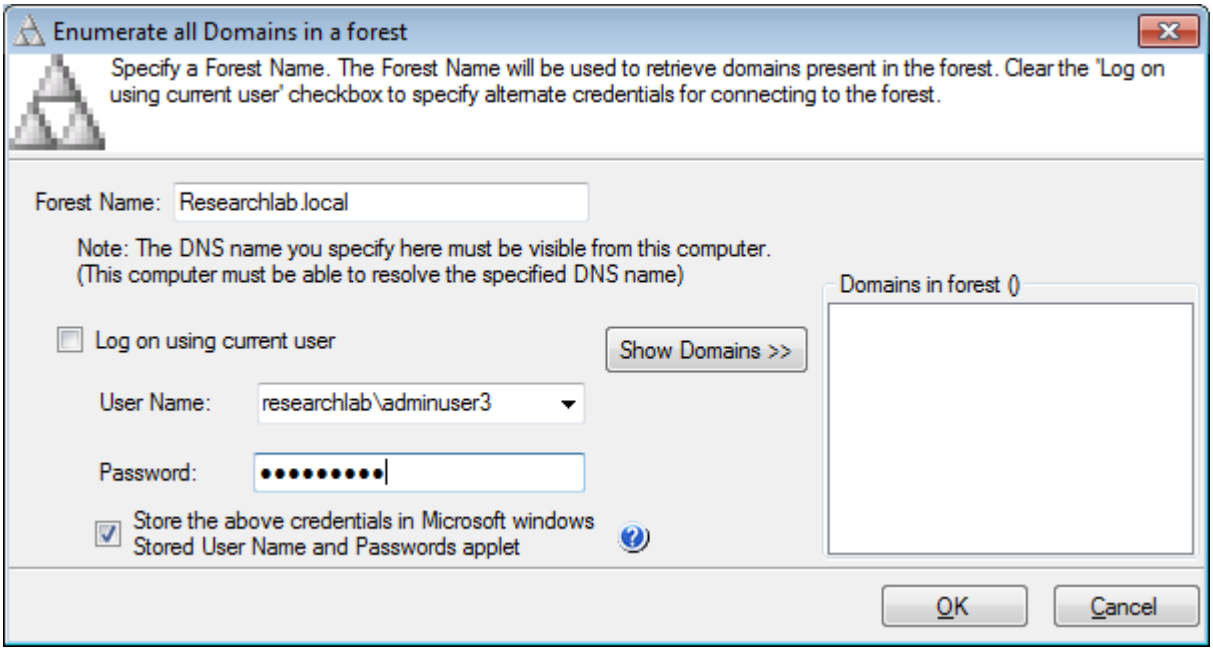
1. Launch Domain Credentials window.

2. In the Domain Credentials window, click to add domains from forest button to add domains in the forest to the list.

3. The Add domains from forest connection dialog will be displayed as shown below:


Enumerate all Domains in a forest
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.
Forest Name:
Note: The DNS name you specify here must be visible from this computer.
(This computer must be able to resolve the specified DNS name)
Domains in forest ()
Log on using current user
Show Domains >>
User Name:
RD54\Administrator
Password:
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
OK
Cancel

Enter the name of a forest.

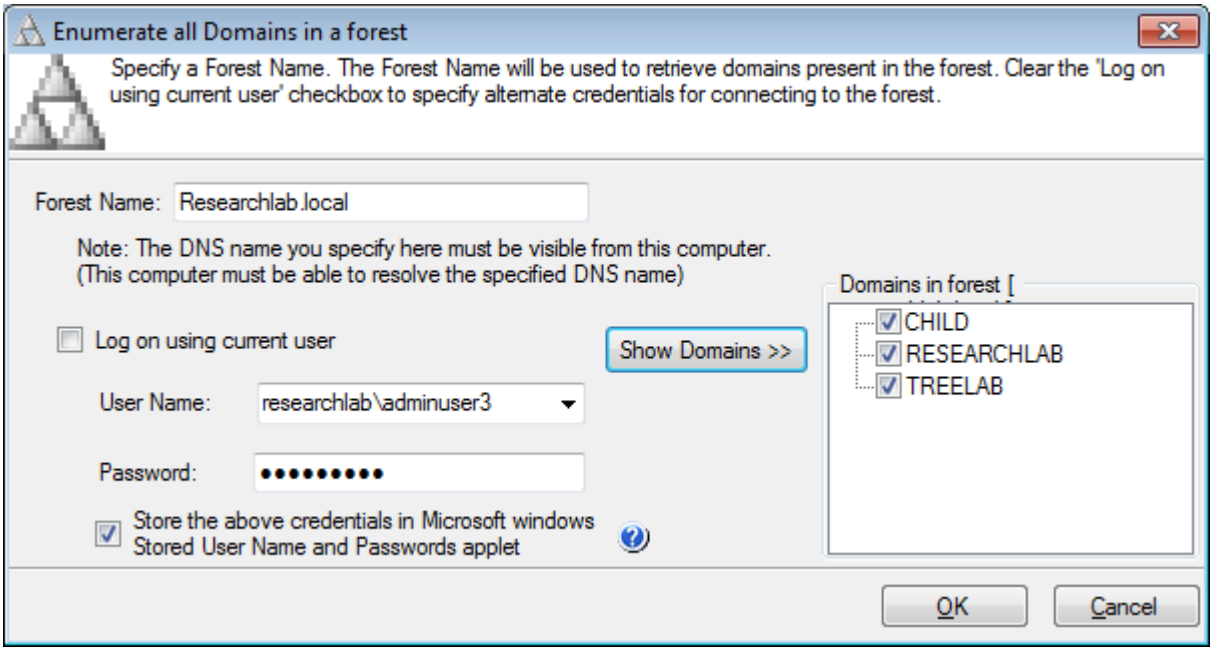

Enumerate all Domains in a forest
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.
Forest Name:
Researchlab.local
Note: The DNS name you specify here must be visible from this computer.
(This computer must be able to resolve the specified DNS name)
Domains in forest ()
Log on using current user
Show Domains >>
User Name:
researchlab\adminuser3
Password:
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
OK
Cancel

4. Specify user name and the corresponding password to connect to the specified forest.

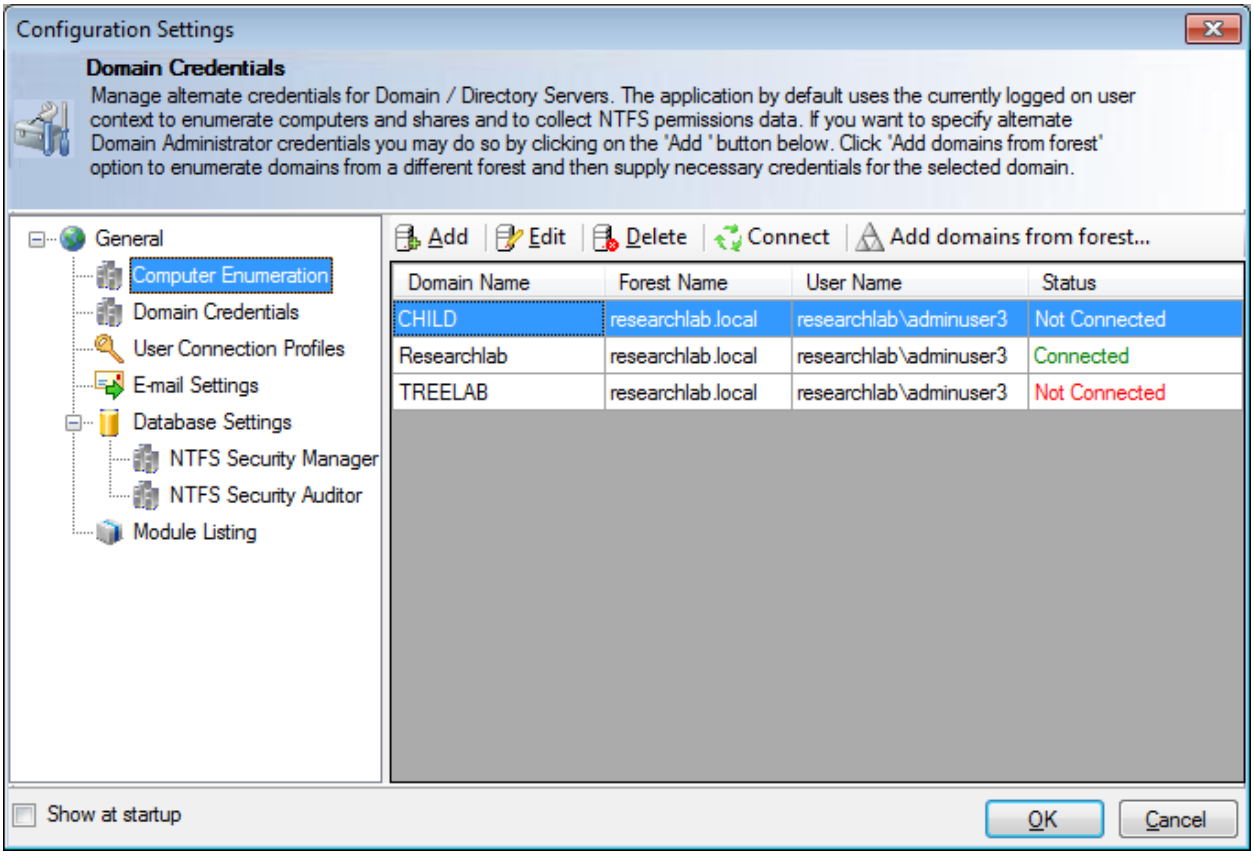
Store the above user credential in **Microsoft Windows Stored User Names and Passwords applet** - NTFS Security Management Suite 2014 allows the user to enter different user credentials to connect to the forest. Uncheck the checkbox 'Log on using current user' if you like to connect to the forest using a different user context.

NTFS Security Management Suite 2014 will store the user credential to connect to forest in the Microsoft Windows Stored User Names and Passwords applet / Credential Manager for security reasons. The stored user profile is tied to the user context (currently logged on user account) in which the profile is created.

5. Click 'Show Domains' button to add the domains in the specified forest to the list and select the desired domains in the list. Click OK to add the selected domains to the Domain Credentials list as shown below.


Enumerate all Domains in a forest
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.
Forest Name: Researchlab.local
Note: The DNS name you specify here must be visible from this computer.
(This computer must be able to resolve the specified DNS name)
Log on using current user
Show Domains >>
User Name: researchlab\adminuser3
Password: ••••••••••
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
Domains in forest [
CHILD
RESEARCHLAB
TREELAB
OK
Cancel

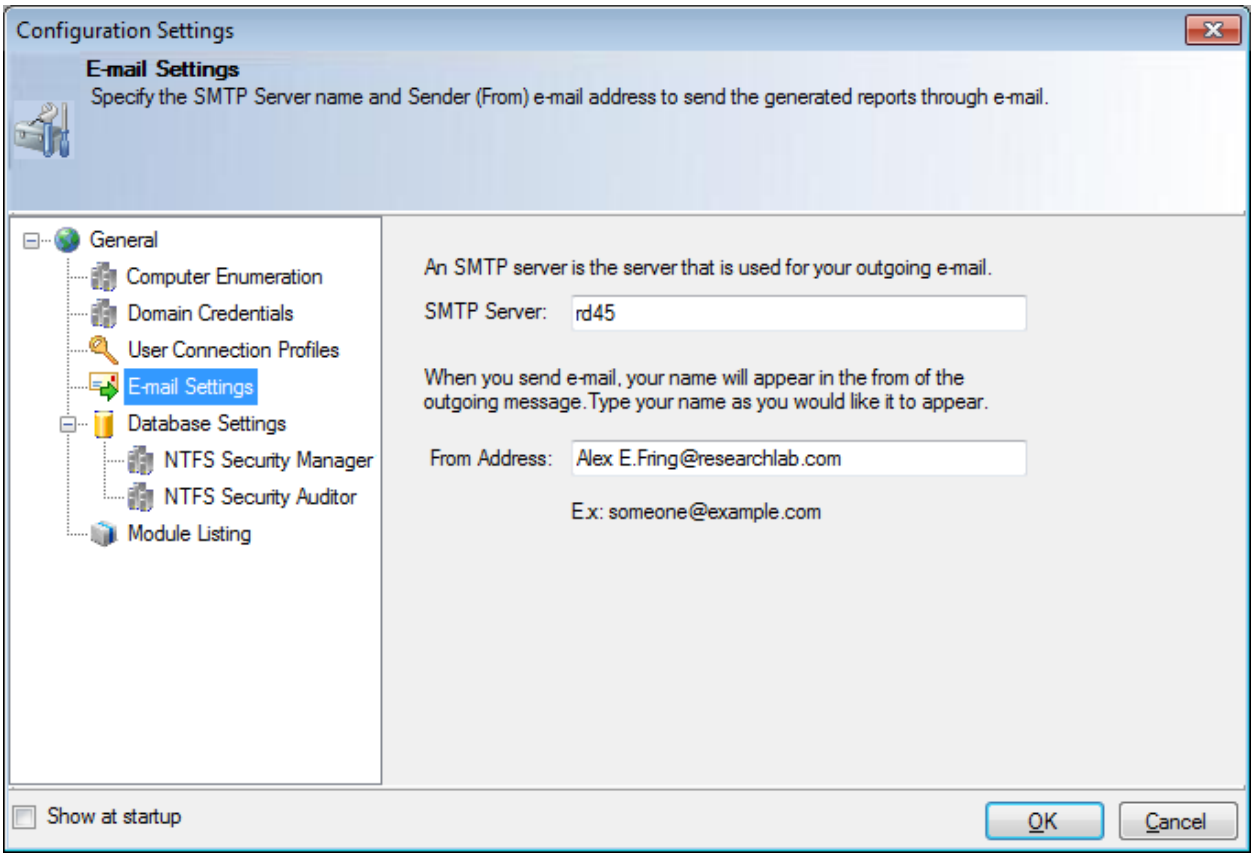
6. NTFS Security Management Suite 2014 will add the selected domains to the Domain Credentials list.



Configure SMTP Server

NTFS Security Management Suite 2014 provides the option to e-mail the reports generated. For e-mailing reports, NTFS Security Management Suite 2014 requires SMTP Server, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the e-mail report format. NTFS Security Management Suite 2014 maintains a single SMTP Server and a From E-mail Address for use by all reports. You can specify a separate set of To e-mail addresses (recipients), e-mail report format, subject and body of the message for each reports.

You can set SMTP Server and From Address by clicking Configuration -> Configuration Settings in the NTFS Security Management Suite 2014 main application window, as shown below:


Configuration Settings
E-mail Settings
Specify the SMTP Server name and Sender (From) e-mail address to send the generated reports through e-mail.
General
Computer Enumeration
Domain Credentials
User Connection Profiles
E-mail Settings
Database Settings
NTFS Security Manager
NTFS Security Auditor
Module Listing
An SMTP server is the server that is used for your outgoing e-mail.
SMTP Server:
rd45
When you send e-mail, your name will appear in the from of the outgoing message. Type your name as you would like it to appear.
From Address:
Alex E.Fring@researchlab.com
E.x: someone@example.com
Show at startup
OK
Cancel

User Connection Profiles

NTFS Security Management Suite 2014 creates a user profile in **Windows Stored User Names and Passwords** applet / **Credential Manager**, in order to store the domain user context for enumerating servers using ADSI.

The stored user profile will be useful for generating reports using NTFS Security Management Suite 2014 under the following scenarios:

- Using an alternate user account to connect to the domain to retrieve servers using ADSI.
- Providing credentials that have sufficient rights to enumerate shares present in computers within a domain.

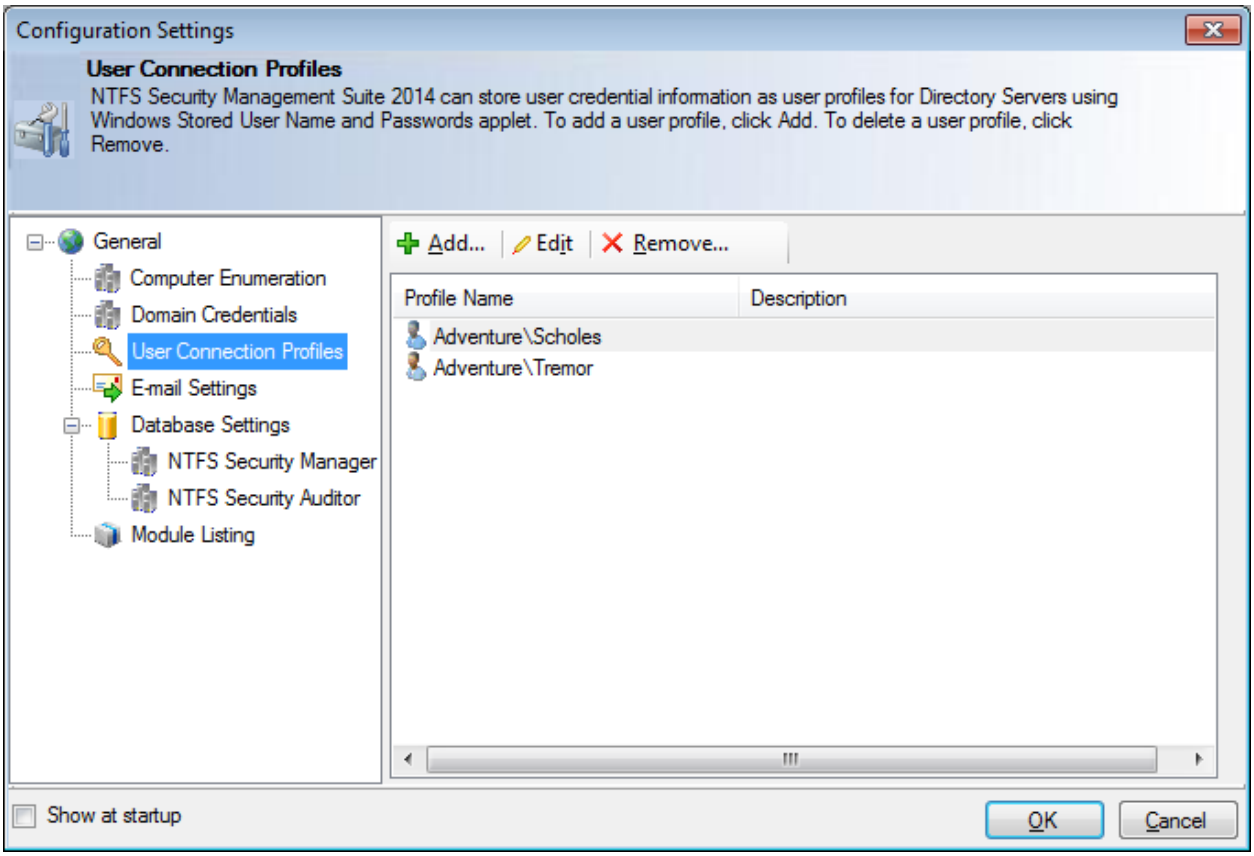
The stored user profile persists for all subsequent logon sessions on the same computer where NTFS Security Management Suite 2014 is installed. The stored user profiles are visible to the application under other logon sessions on the same computer.

The stored user profile created by NTFS Security Management Suite 2014 is restricted to the Windows User Profile context. If the Windows User Profile is maintained locally, NTFS Security Management Suite 2014 stored user profile is accessible only by the same user in the same computer. If the user who creates NTFS Security Management Suite 2014 stored user profile, has a Roaming user account in the enterprise, the NTFS Security Management Suite 2014 stored user profile can be accessed by the same user in any computer in the Windows enterprise.

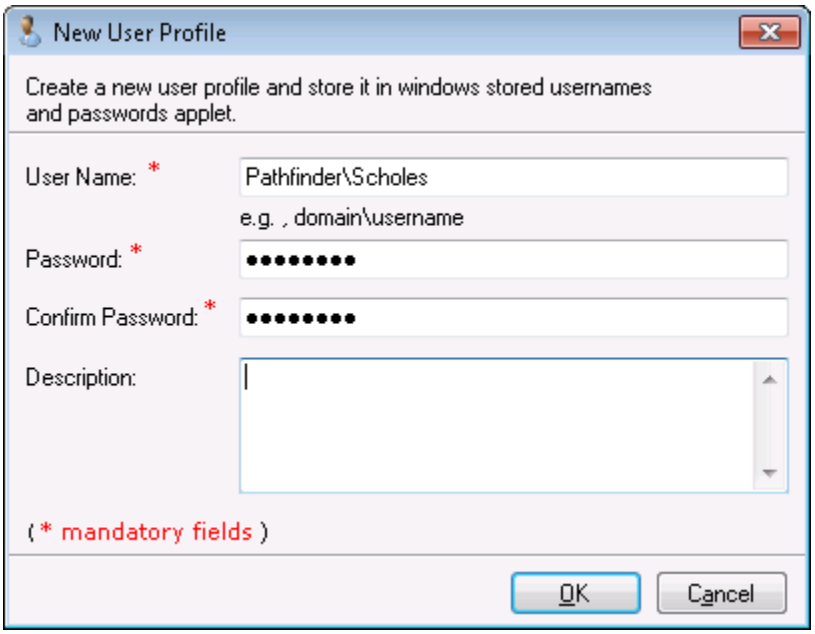
The stored user profile is a generic credential of **Windows Stored User Names and Passwords** applet / **Credential Manager** and can be used by the application only. The credential information is stored securely in a 256 bit encrypted format in **Windows Stored User Names and Passwords** applet / **Credential Manager**.

The stored user profile corresponding to the user account will be used by the application in order to connect to the domain, if 'Use ADSI' is selected in NTFS Security Management Suite 2014 Enumeration Settings.

Using the Connection Profile dialog show below, new profile can be created and available profiles can be removed from the profiles list.



Click **Add** button to add a new profile and a dialog will appear as shown below:



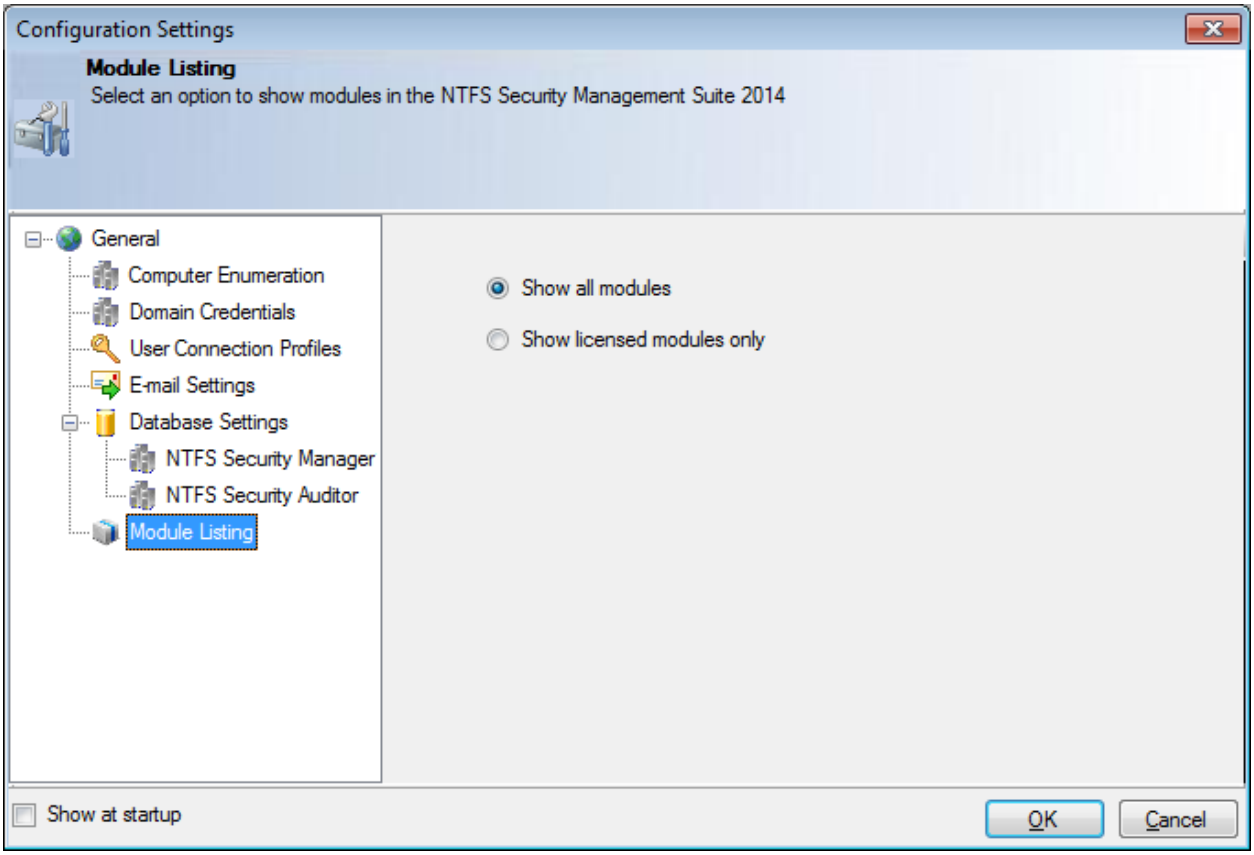
Click **Edit** button in the Connection Profile dialog to edit available profiles.

Click **Remove** button in the Connection Profile dialog to remove available profiles.

Module Listing

This option allows you to view/hide the license expired modules in the NTFS Security Management Suite 2014.

You can access the **Module Listing** option by clicking Configuration -> Configuration Settings in the NTFS Security Management Suite 2014 main application window and selecting "Module Listing" node as shown below:



- Use the **Show all modules** option to view all available modules in the NTFS Security Management Suite 2014.
- Use the **Show licensed modules only** option to hide the license expired modules in the NTFS Security Management Suite 2014.

NTFS Security Auditor

Standard Reports

Built-in Reports

DAC Reports

Security Viewer

Power Search

Power Export

Built-in Reports

About Built-in Reports

How to view Built-in Permissions Reports?

How to view Built-in Reports for Shares and Resources?

About Built-in Reports

Built-in reports are a set of predefined reports that are based on some of the common tasks in NTFS permissions reporting. Built-in reports are easy to use because of the built-in queries that speed up the report generation process.

The built-in reports feature provides reports in the following categories:

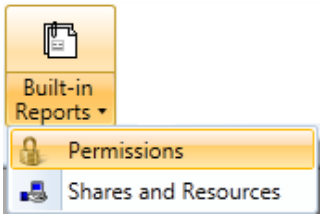
Permissions Reports

Shares and Resources

How to view Built-in Permissions Reports?

Permissions Reports

Permissions Reports includes reports that focus solely on reporting the access permissions assigned to users and groups on objects such as folders etcetera.

Click on 

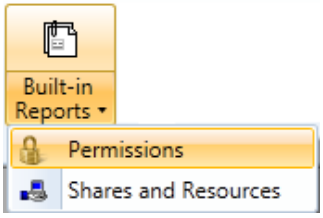
button under Built-in Reports.

List of Permissions Reports:

Report Name	Description
List of permissions for specific users and groups on folders	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
List of permissions for folders	Reports the permissions associated with a selected set of folders.
List of permissions for specific users and groups on files	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.
List of permissions for files	Reports the permissions associated with files under a selected set of folders.
List of all permissions for folders (Inherit & Explicit)	Reports the permissions for users assigned in the folders directly and inherited by means of nested groups.
List of effective permissions for users and groups on folders	Reports the effective permissions for users and groups for a set of folders.
List of effective permissions for users and groups on files	Reports the effective permissions for users and groups for files available in a set of folders.
List of effective permissions for specific users and groups on folders	Reports the effective permissions for specific users and groups available in a set of folders.
List of effective permissions for specific users and groups on files	Reports the effective permissions for specific users and groups for files available in a set of folders.

List of permissions for specific users and groups on folders

This report allows you to view folder permissions for specific users and groups.

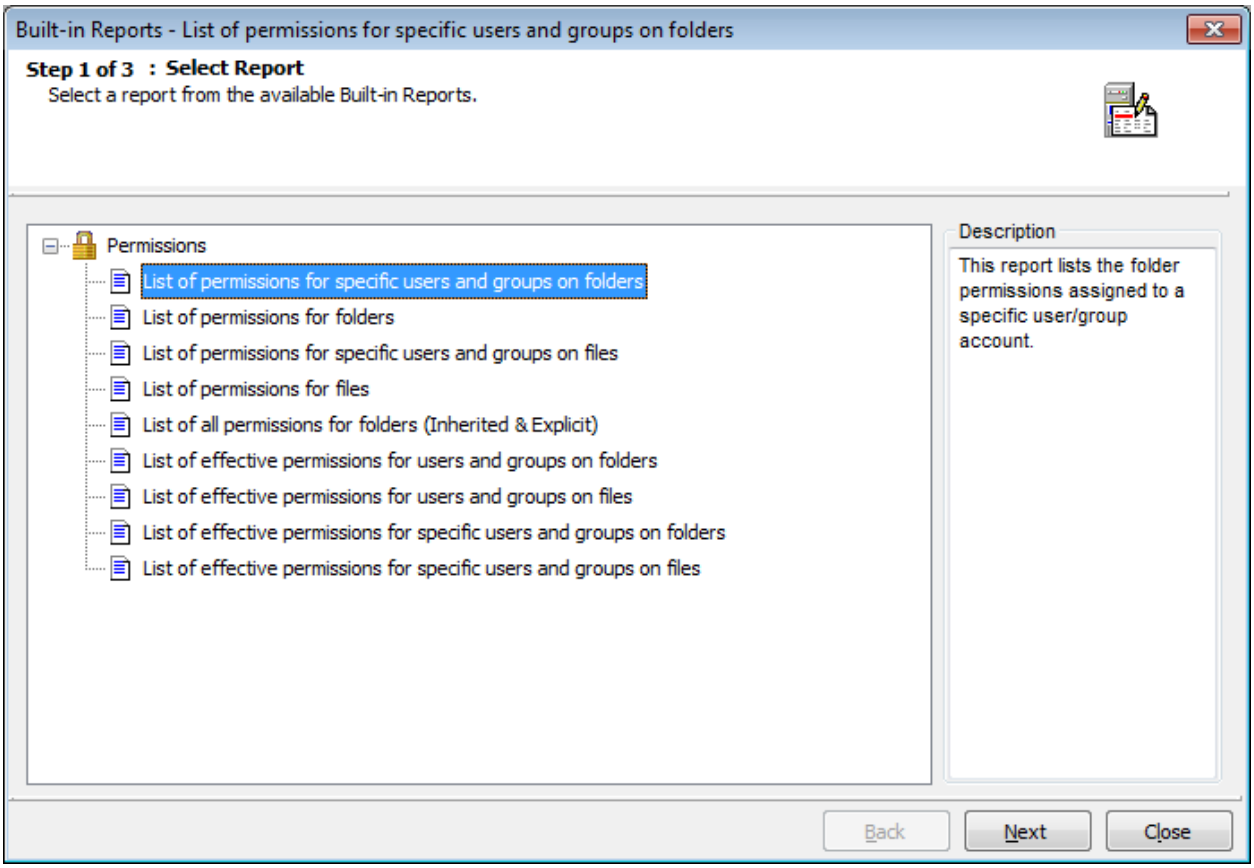
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

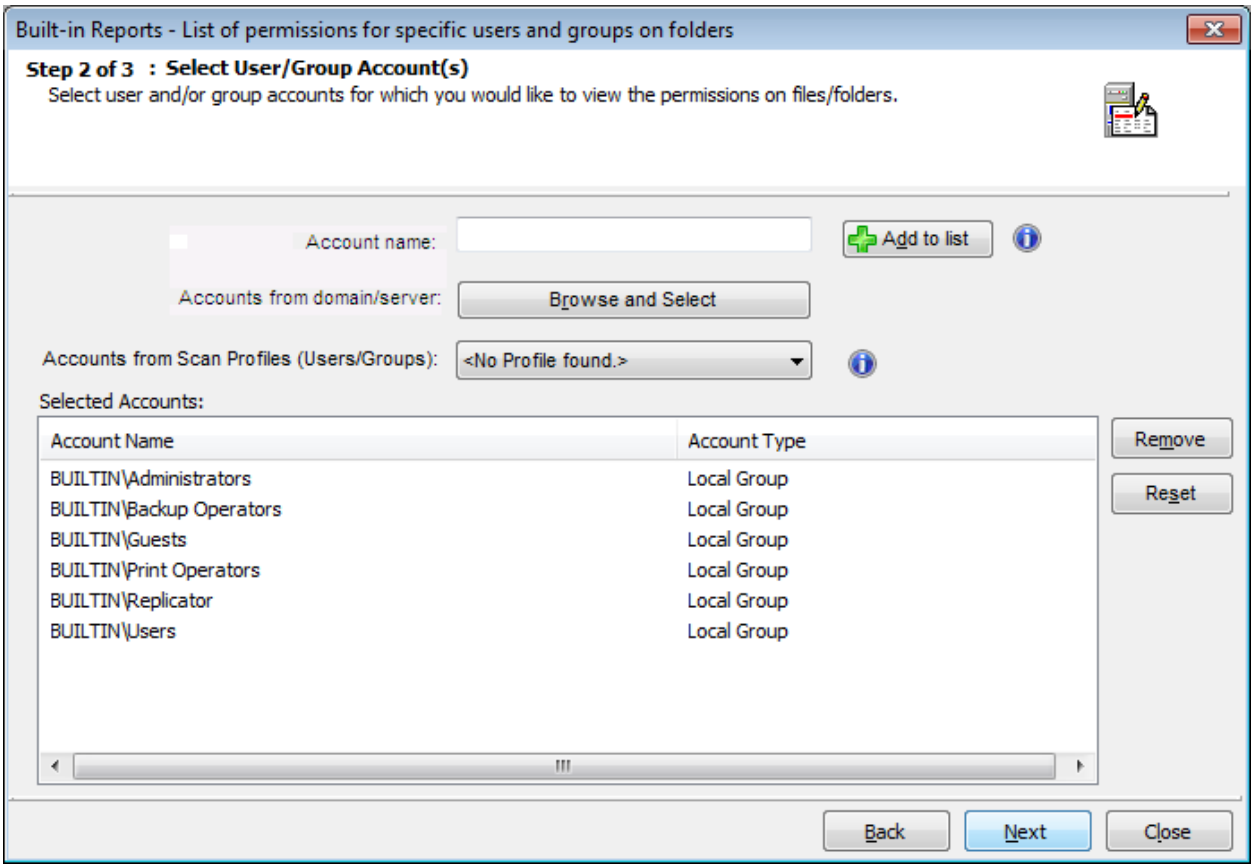
Select the report to be generated. Only one report can be generated at a time.


Built-in Reports - List of permissions for specific users and groups on folders
Step 1 of 3 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the folder permissions assigned to a specific user/group account.
Back
Next
Close

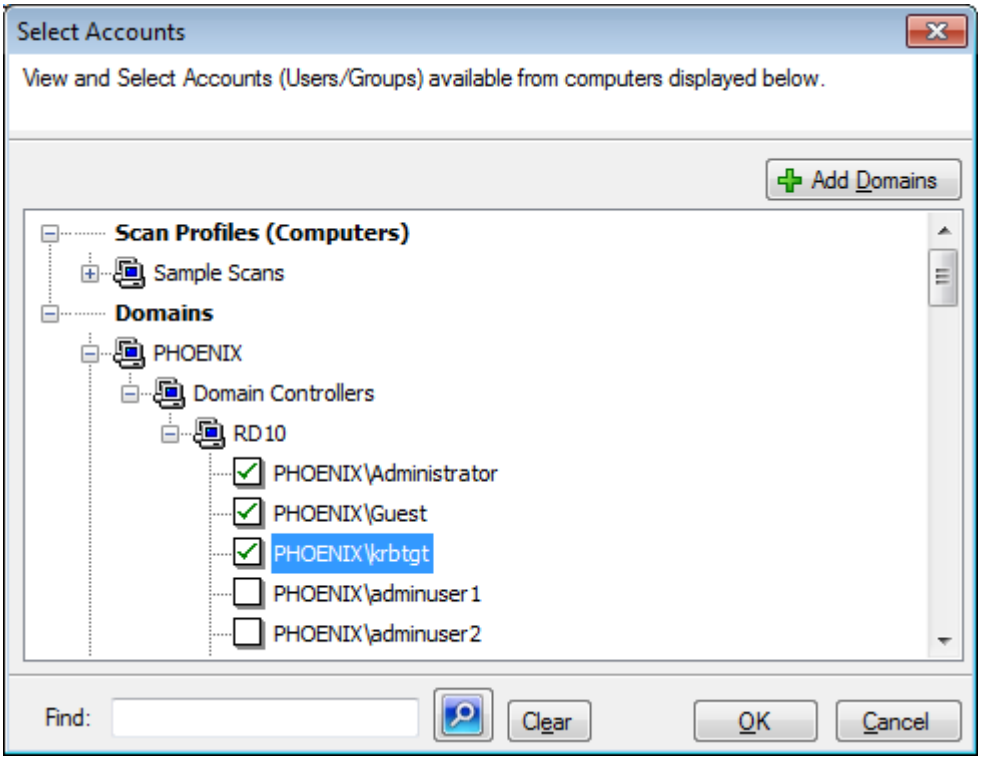
Click **Next** to proceed to the next step.

Step 2: Select User/Group Accounts

Select user and/or group accounts for which you would like to view the permissions for folders/files.



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).

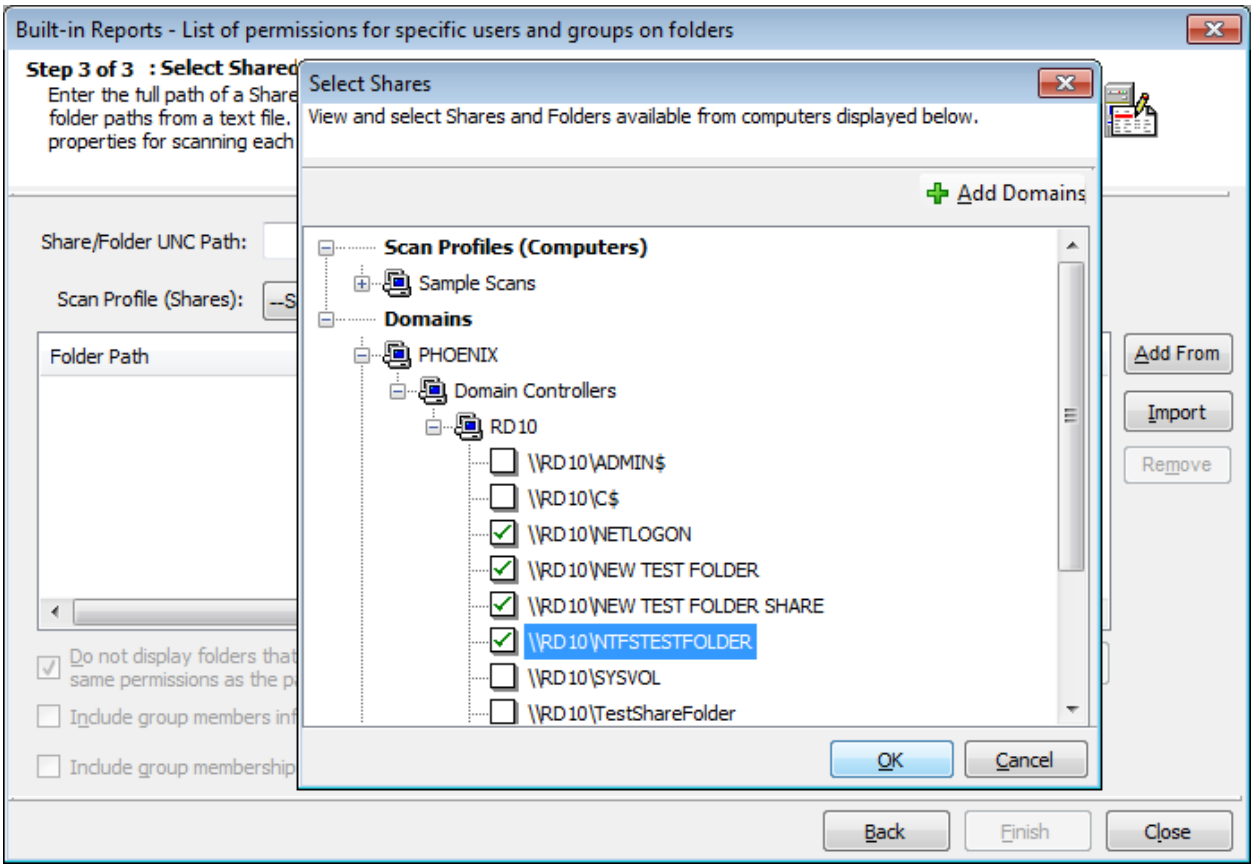


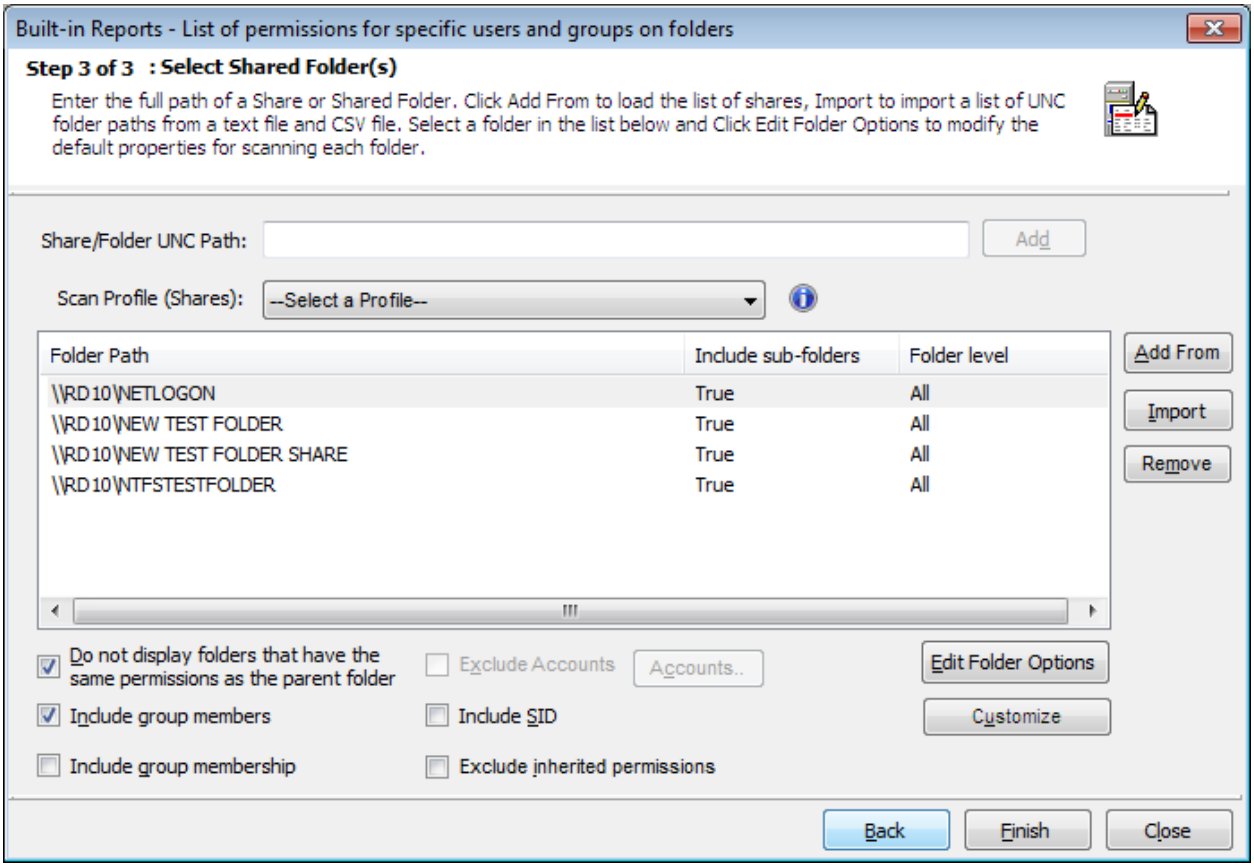
- Use the **Find** option to search desired user/group accounts.

Click **Next** to proceed.

Step 3: Select shared folders

Select one or more servers to retrieve available shares.




Built-in Reports - List of permissions for specific users and groups on folders
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\NTFSTESTFOLDER
True
All
Add From
Import
Remove
Do not display folders that have the same permissions as the parent folder
Exclude Accounts
Accounts..
Edit Folder Options
Include group members
Include SID
Customize
Include group membership
Exclude inherited permissions
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

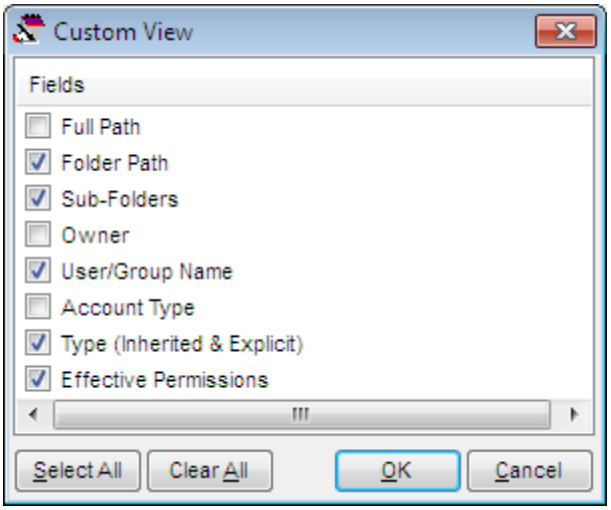
You can select **Include SID** option to include SID value for user in the report.

You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.

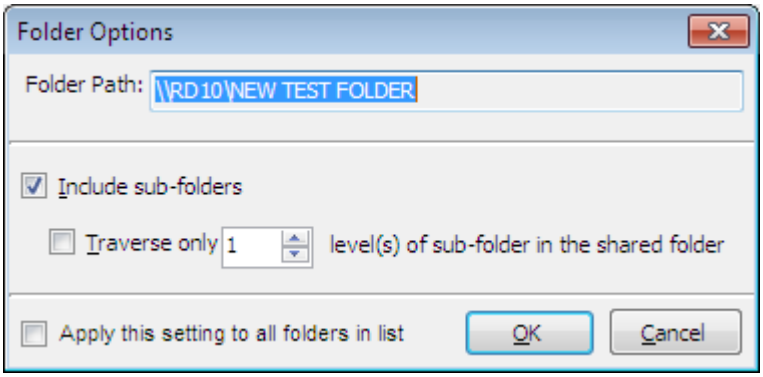
You can select **Include group membership** option to include all membership information of user and group in the report.

You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



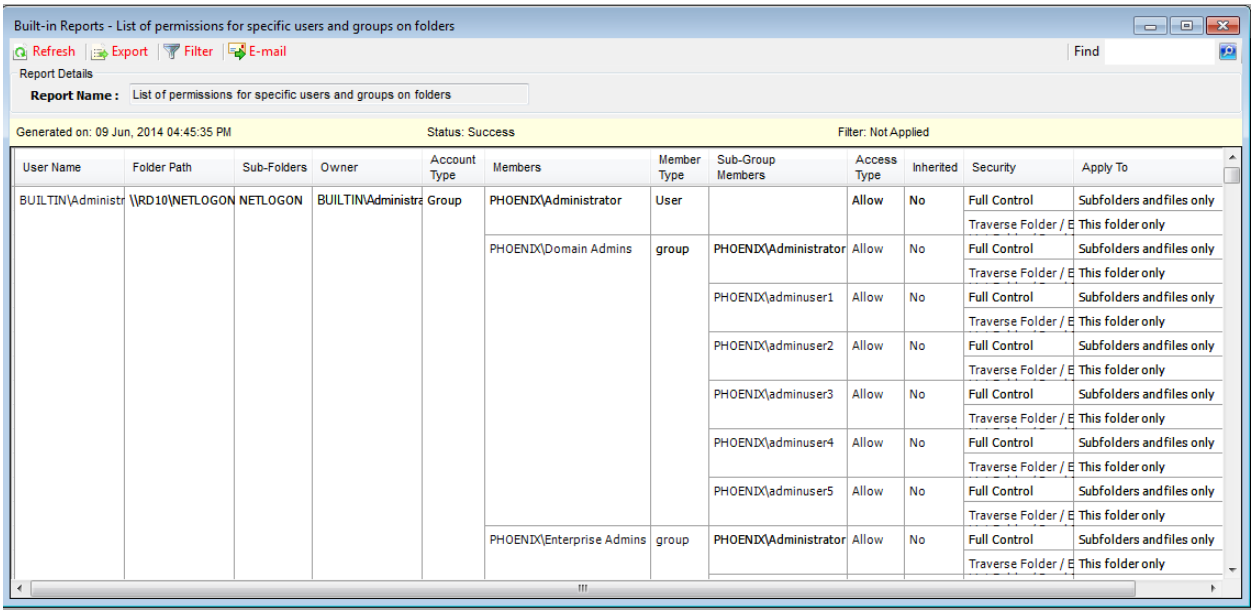
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

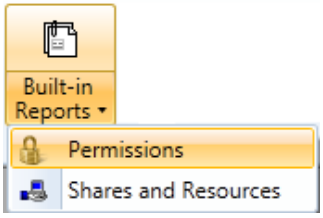
After the data collection process is complete, the report would be generated in a report window as shown below:


Built-in Reports - List of permissions for specific users and groups on folders
Refresh
Export
Filter
E-mail
Find
Report Details
Report Name : List of permissions for specific users and groups on folders
Generated on: 09 Jun, 2014 04:45:35 PM
Status: Success
Filter: Not Applied

User Name	Folder Path	Sub-Folders	Owner	Account Type	Members	Member Type	Sub-Group Members	Access Type	Inherited	Security	Apply To
BUILTIN\Administr	\\RD10\NETLOGON	NETLOGON	BUILTIN\Administra	Group	PHOENIX\Administrator	User		Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
					PHOENIX\Domain Admins	group	PHOENIX\Administrator	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
							PHOENIX\adminuser1	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
							PHOENIX\adminuser2	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
							PHOENIX\adminuser3	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
							PHOENIX\adminuser4	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
							PHOENIX\adminuser5	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only
					PHOENIX\Enterprise Admins	group	PHOENIX\Administrator	Allow	No	Full Control	Subfolders andfiles only
										Traverse Folder / E	This folder only

List of permissions for folders

This report allows you to view the associated permissions for specific folders.

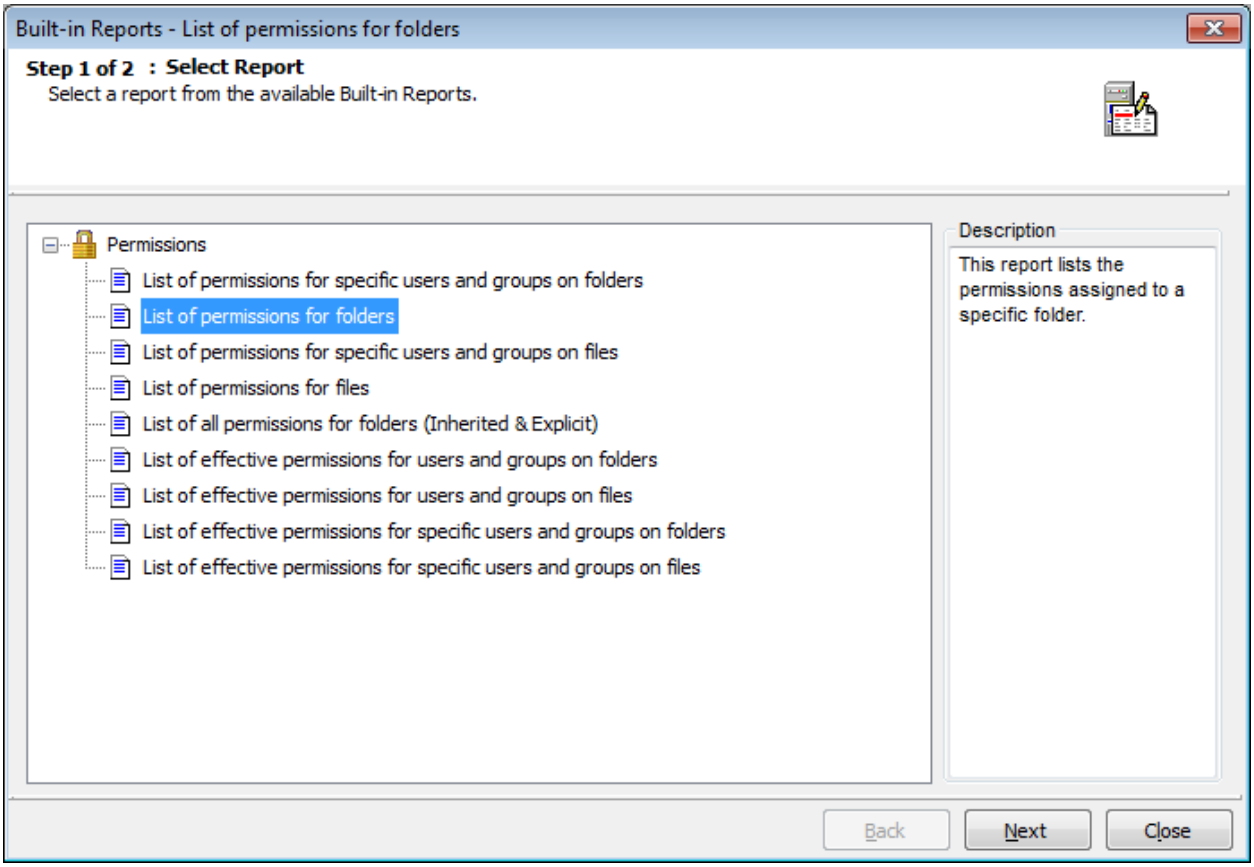
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

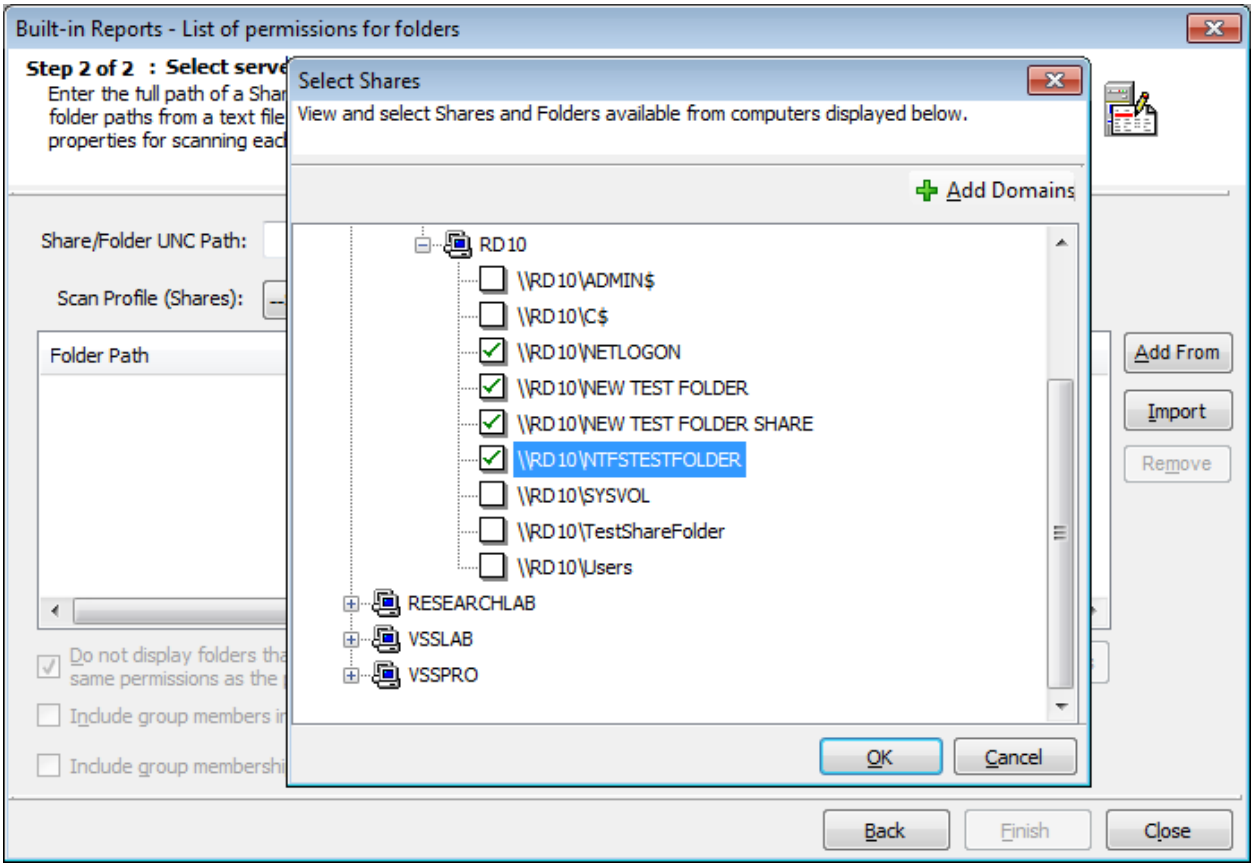
Select the report to be generated. Only one report can be generated at a time.

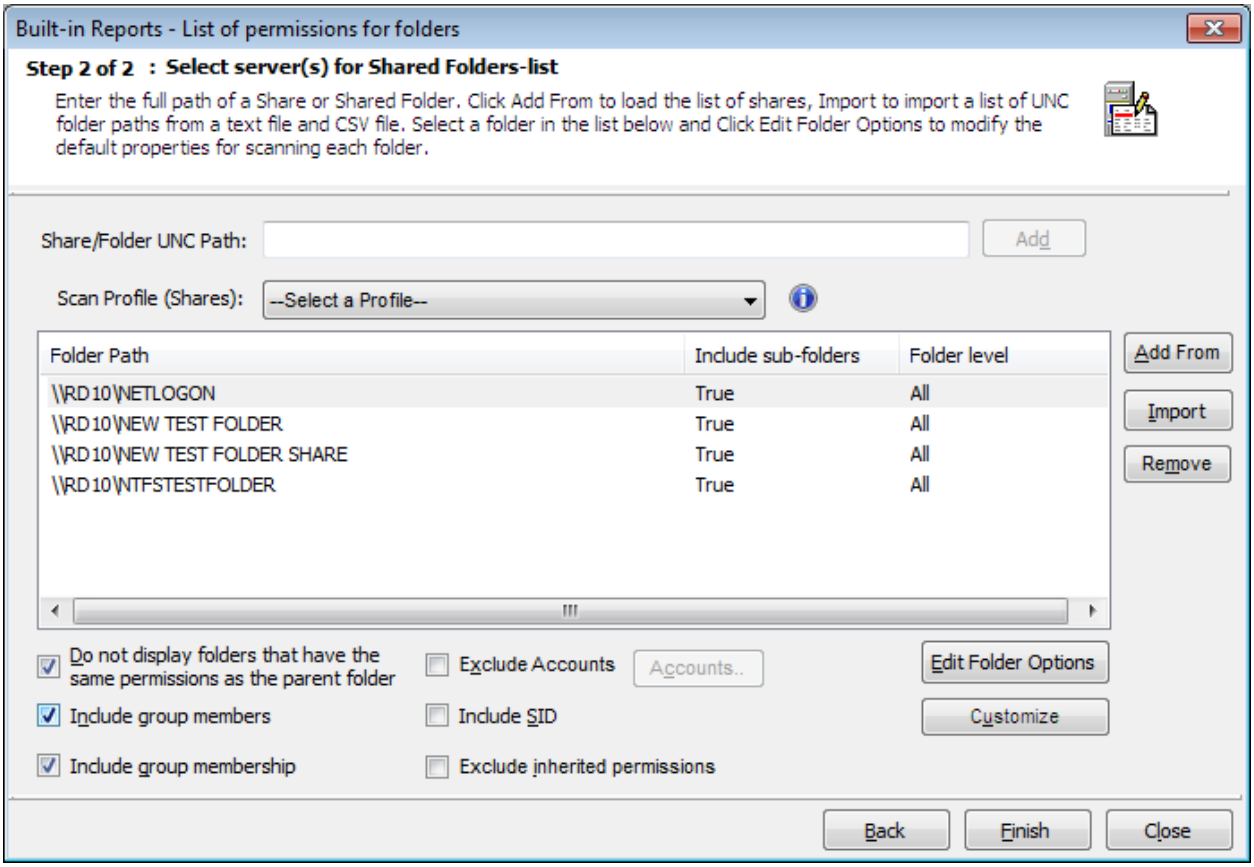

Built-in Reports - List of permissions for folders
Step 1 of 2 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the permissions assigned to a specific folder.
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares


Built-in Reports - List of permissions for folders
Step 2 of 2 : Select serve
Enter the full path of a Shar
folder paths from a text file
properties for scanning eac
Share/Folder UNC Path:
Scan Profile (Shares):
Folder Path
Add From
Import
Remove
Do not display folders tha
same permissions as the
Include group members in
Include group membershi
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Add Domains
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\TestShareFolder
\\RD10\Users
RESEARCHLAB
VSSLAB
VSSPRO
OK
Cancel

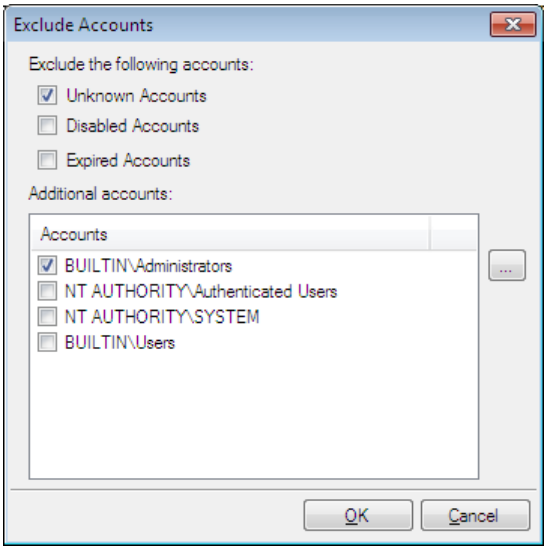


You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

If you want to exclude specific accounts from reporting, select **Exclude Accounts** option. Click **Accounts...** button to launch **Exclude Accounts** window, as shown below:



Select the accounts for which you want to exclude and click OK.

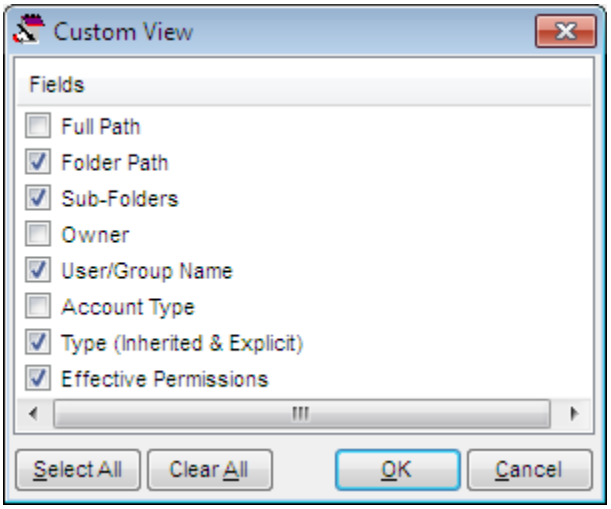
You can select **Include SID** option to include SID value for user in the report.

You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.

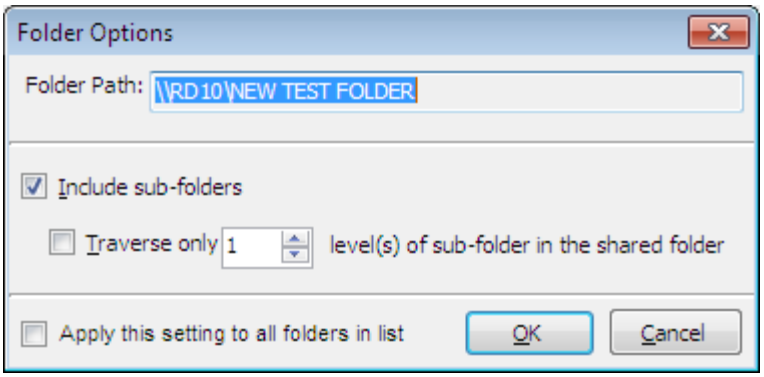
You can select **Include group membership** option to include all membership information of user and group in the report.

You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



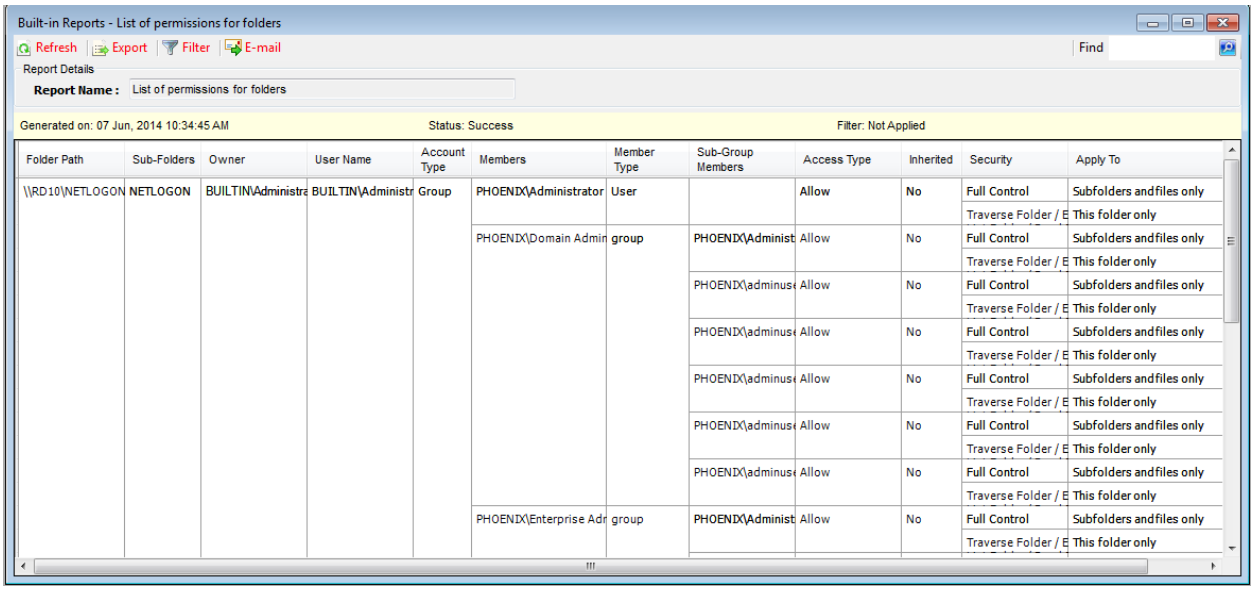
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.


Folder Options
Folder Path: \\RD10\NEW TEST FOLDER
Include sub-folders
Traverse only 1 level(s) of sub-folder in the shared folder
Apply this setting to all folders in list
OK
Cancel

Click **OK** to proceed.

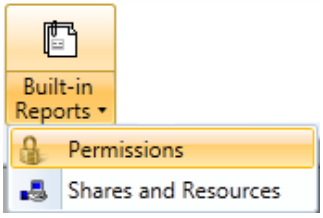
Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



List of permissions for specific users and groups on files

This report allows you to view file permissions for specific users and groups.

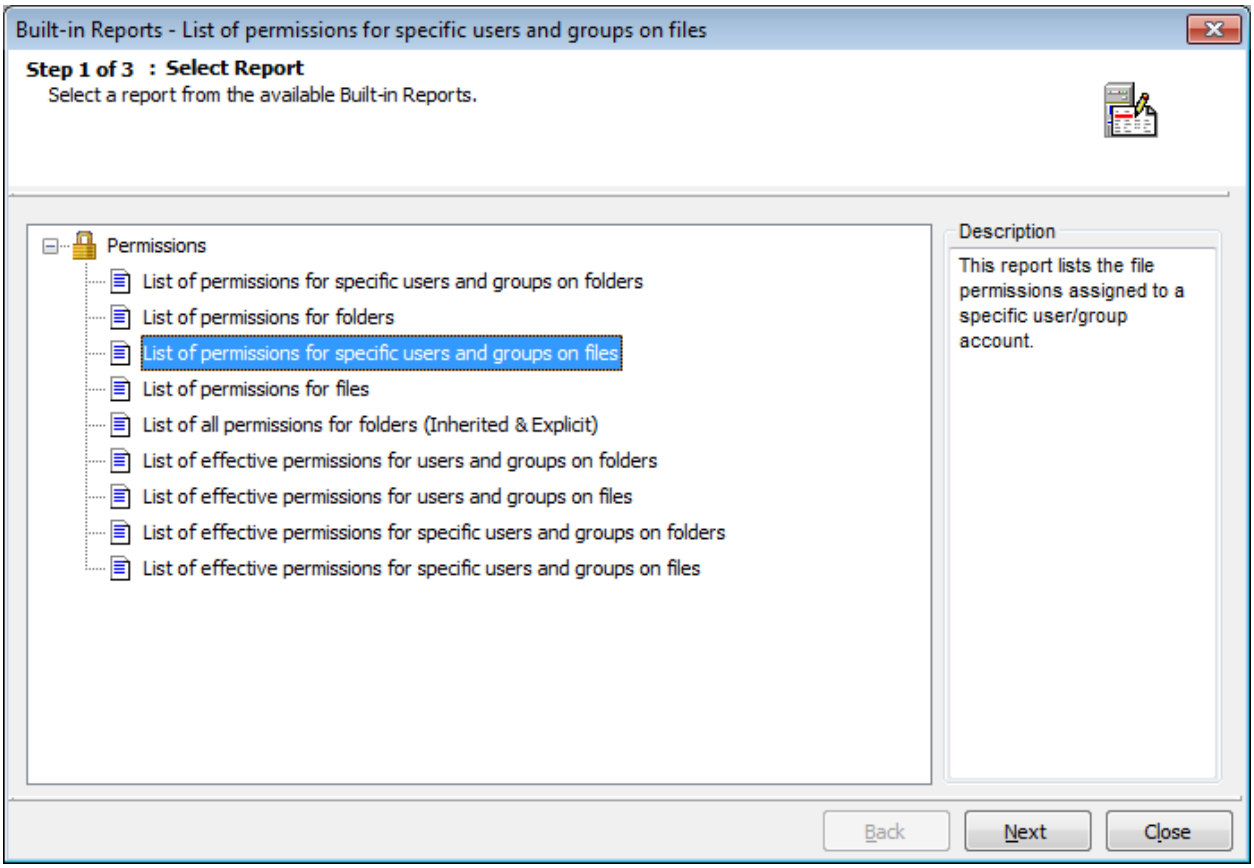
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

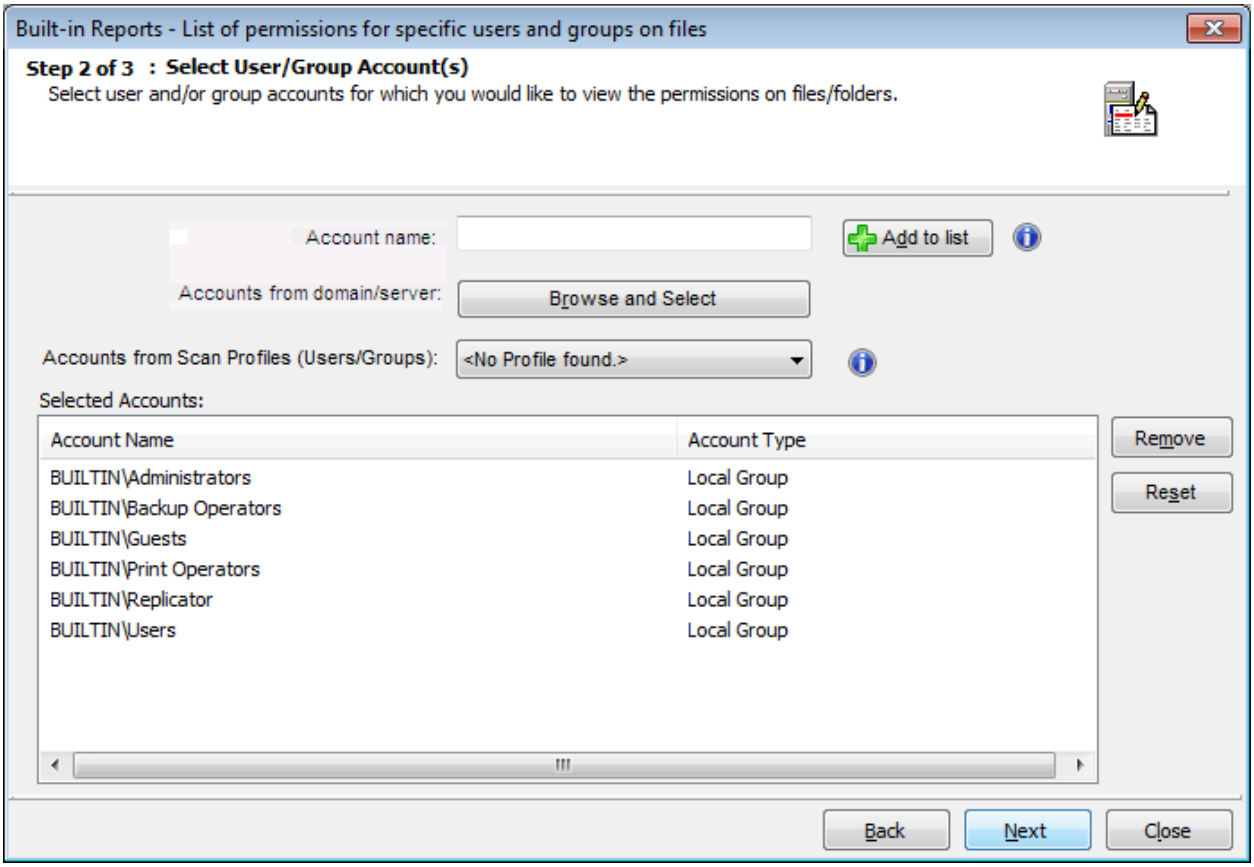
Select the report to be generated. Only one report can be generated at a time.


Built-in Reports - List of permissions for specific users and groups on files
Step 1 of 3 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the file permissions assigned to a specific user/group account.
Back
Next
Close

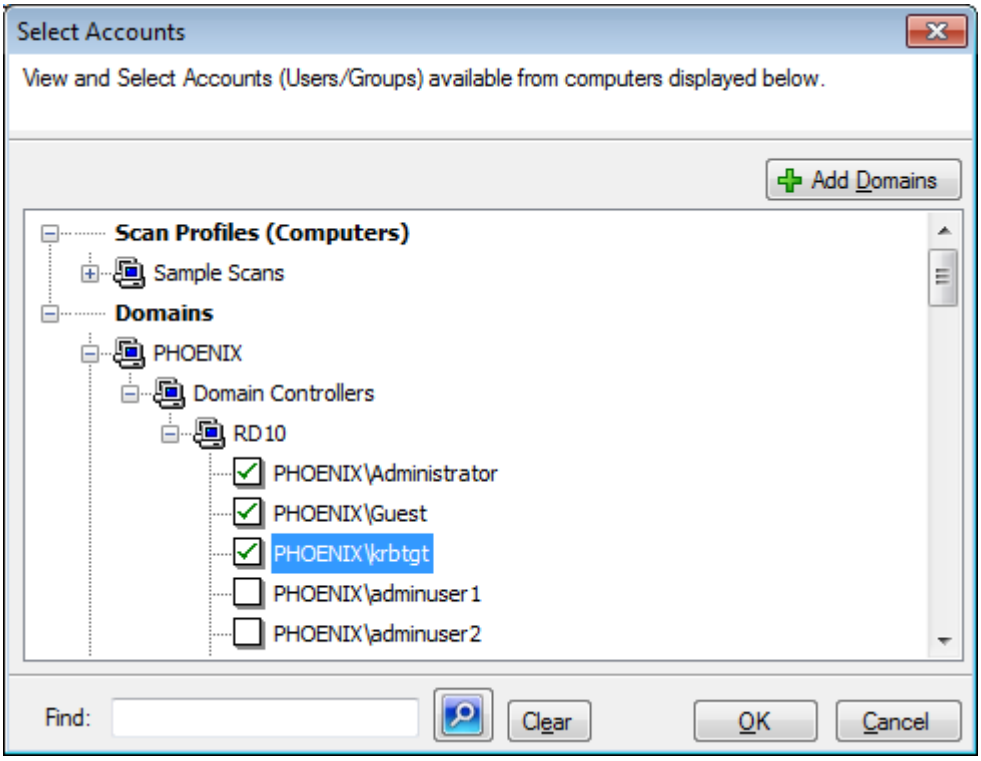
Click **Next** to proceed to the next step.

Step 2: Select User/Group Accounts

Select user and/or group accounts for which you would like to view the permissions for folders/files.



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).

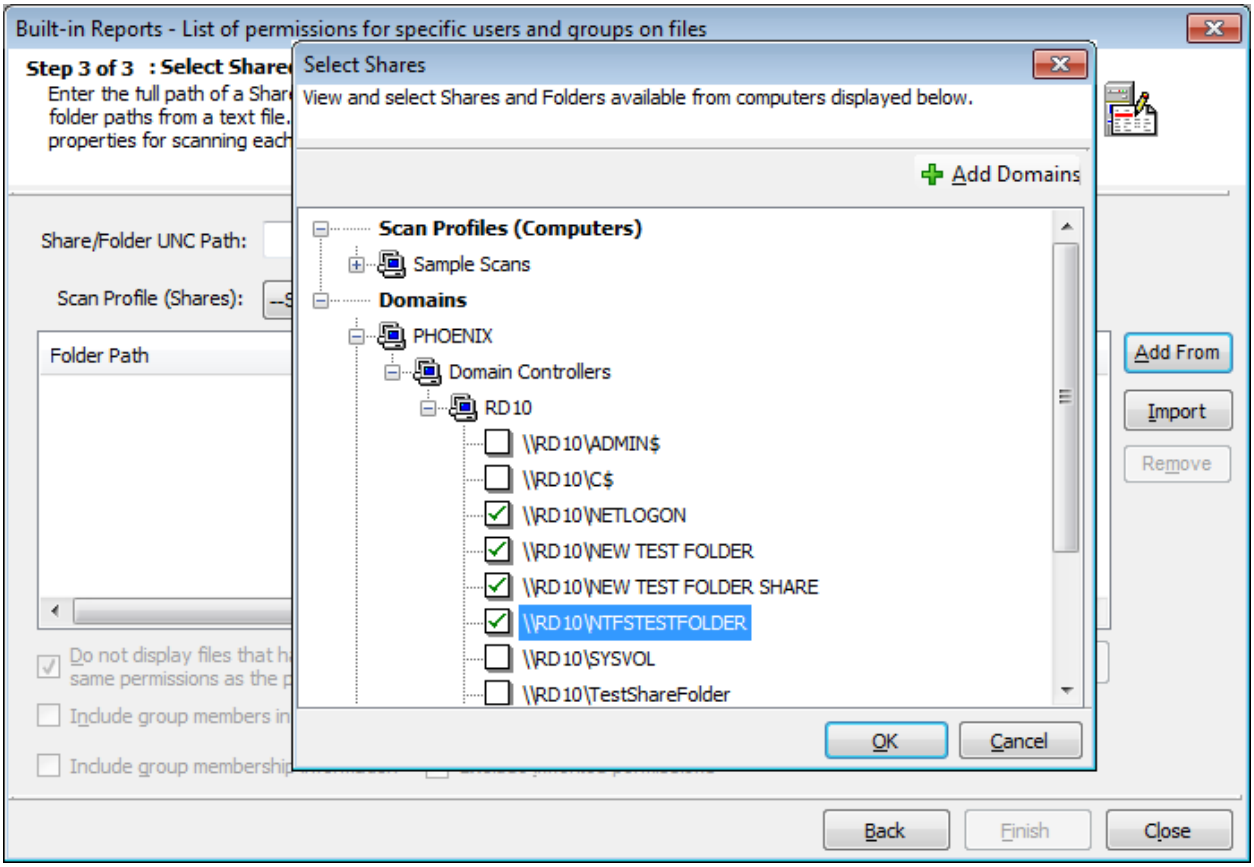


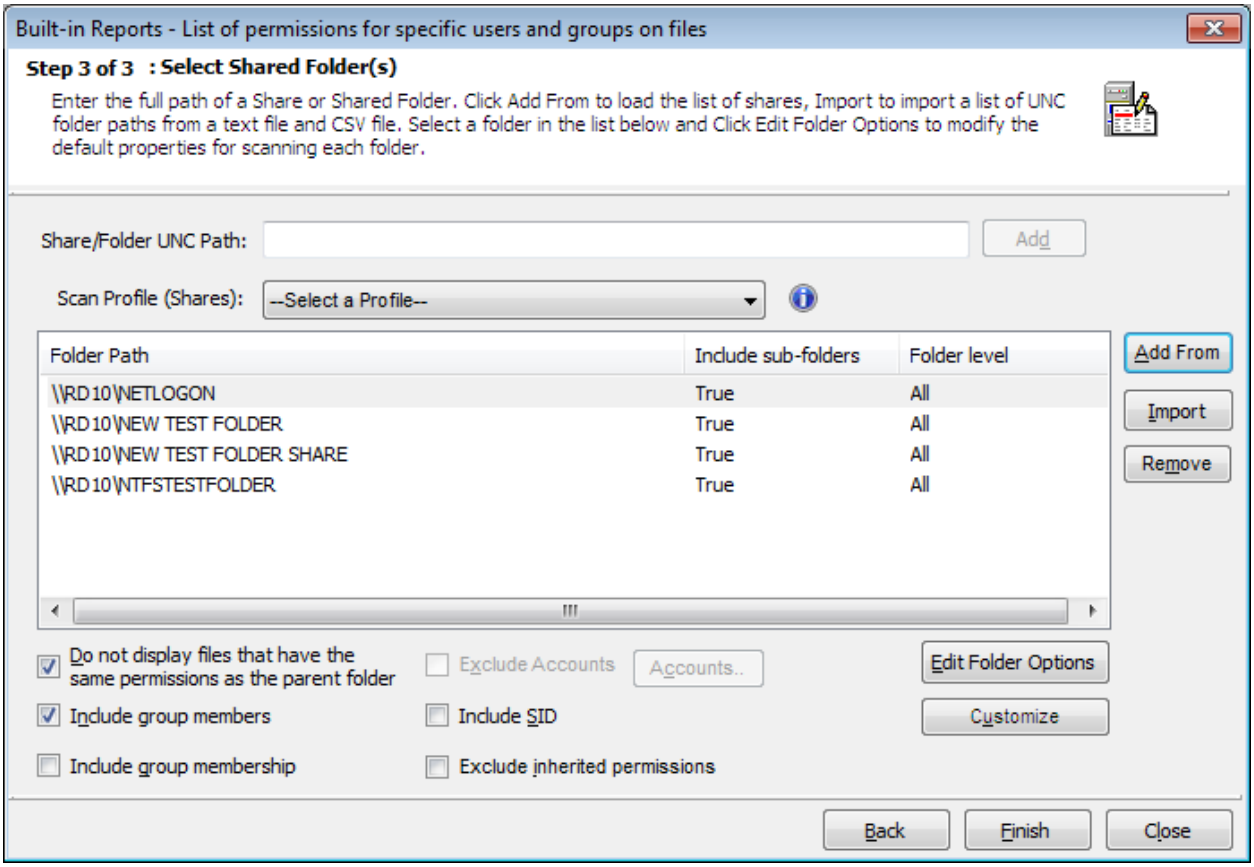
- Use the **Find** option to search desired user/group accounts.

Click **Next** to proceed.

Step 3: Select shared folders

Select one or more servers to retrieve available shares.


Built-in Reports - List of permissions for specific users and groups on files
Step 3 of 3 : Select Share
Enter the full path of a Shar
folder paths from a text file.
properties for scanning each
Share/Folder UNC Path:
Scan Profile (Shares):
Folder Path
Add From
Import
Remove
Do not display files that h
same permissions as the p
Include group members in
Include group membership
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Add Domains
Scan Profiles (Computers)
Sample Scans
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\TestShareFolder
OK
Cancel


Built-in Reports - List of permissions for specific users and groups on files
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\NTFSTESTFOLDER
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Exclude Accounts
Accounts..
Edit Folder Options
Include group members
Include SID
Customize
Include group membership
Exclude inherited permissions
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

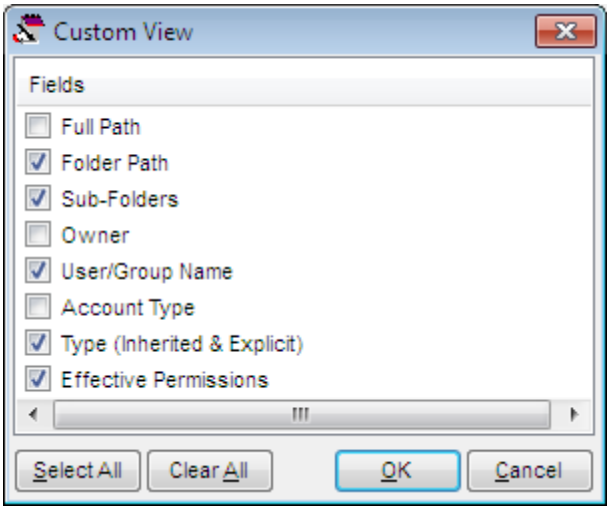
You can select **Include SID** option to include SID value for user in the report.

You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.

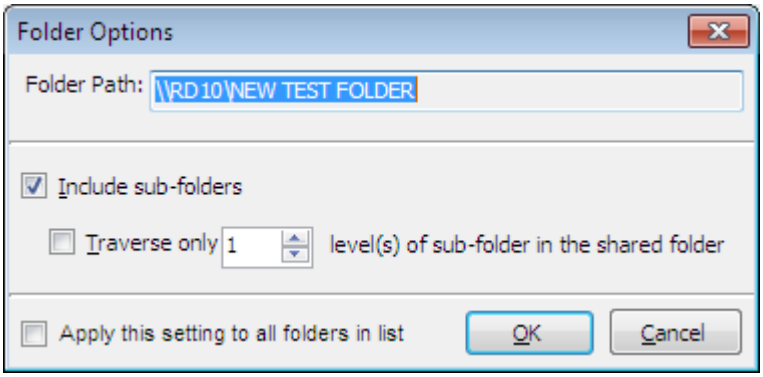
You can select **Include group membership** option to include all membership information of user and group in the report.

You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



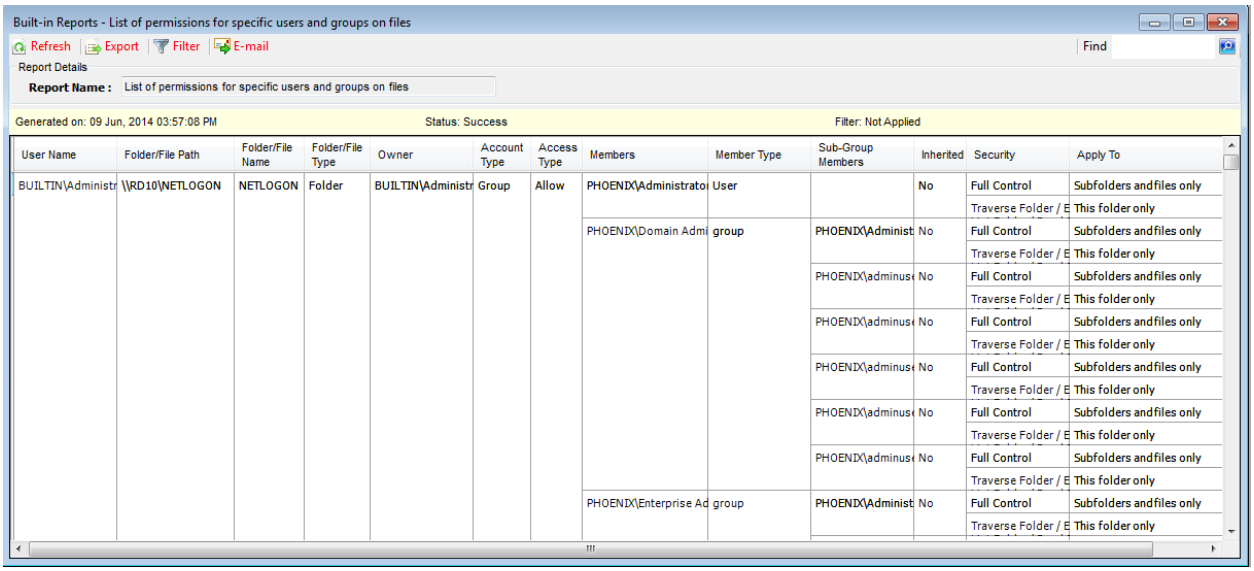
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

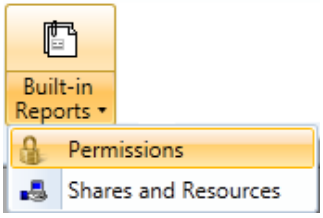
After the data collection process is complete, the report would be generated in a report window as shown below:



User Name	Folder/File Path	Folder/File Name	Folder/File Type	Owner	Account Type	Access Type	Members	Member Type	Sub-Group Members	Inherited	Security	Apply To
BUILTIN\Administr	\\RD10\NETLOGON	NETLOGON	Folder	BUILTIN\Administr	Group	Allow	PHOENIX\Administrato	User		No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
							PHOENIX\Domain Admi	group	PHOENIX\Administ	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
									PHOENIX\adminus	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
									PHOENIX\adminus	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
									PHOENIX\adminus	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
									PHOENIX\adminus	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
									PHOENIX\adminus	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only
							PHOENIX\Enterprise Ad	group	PHOENIX\Administ	No	Full Control	Subfolders andfiles only
											Traverse Folder / E	This folder only

List of permissions for files

This report allows you to view the associated permissions for specific files.

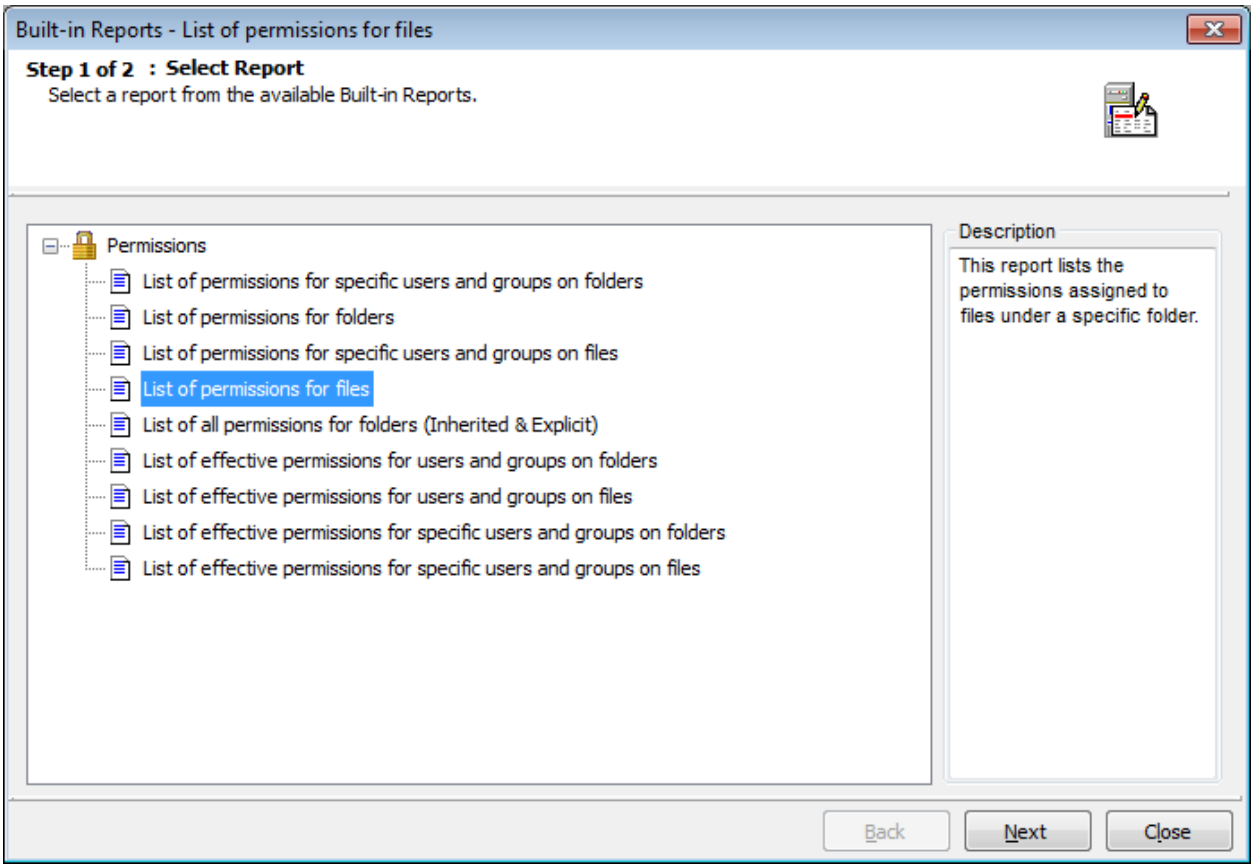
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

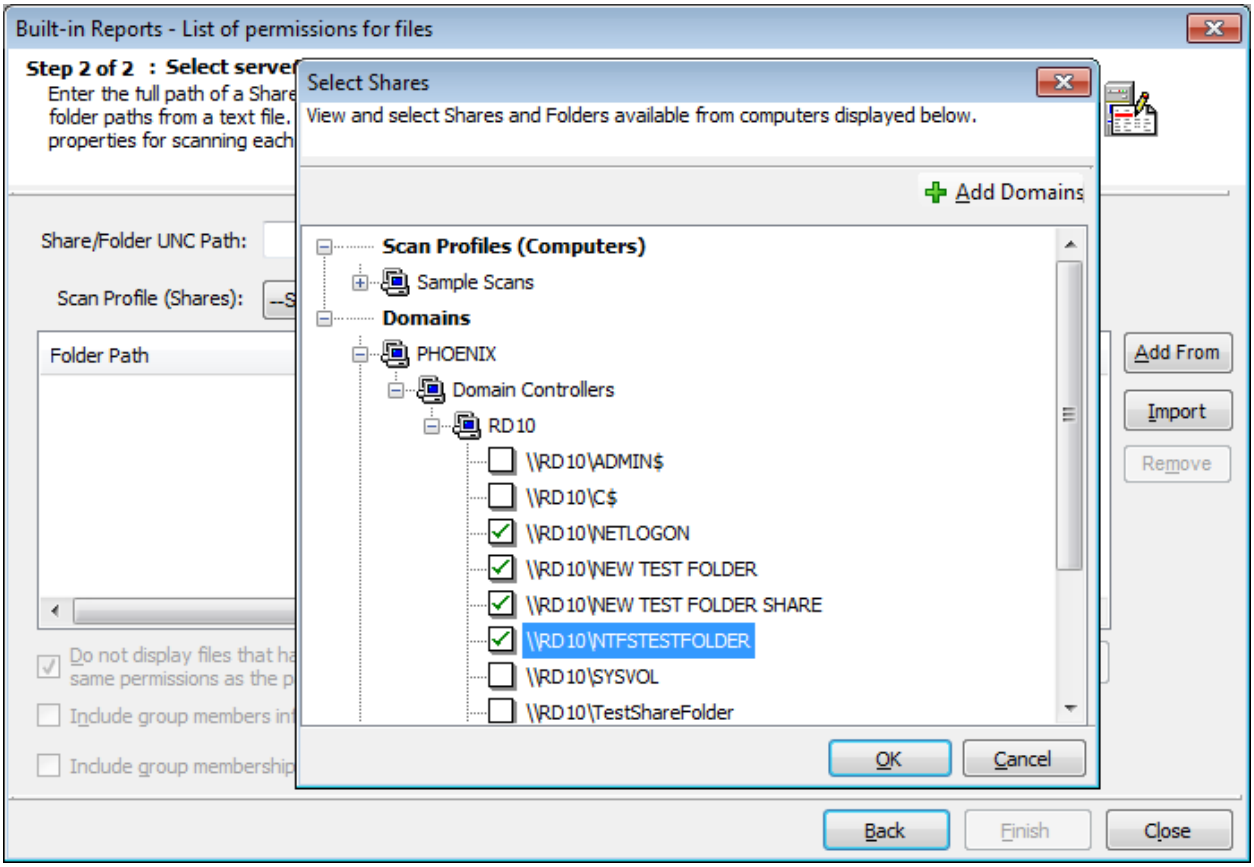
Select the report to be generated. Only one report can be generated at a time.

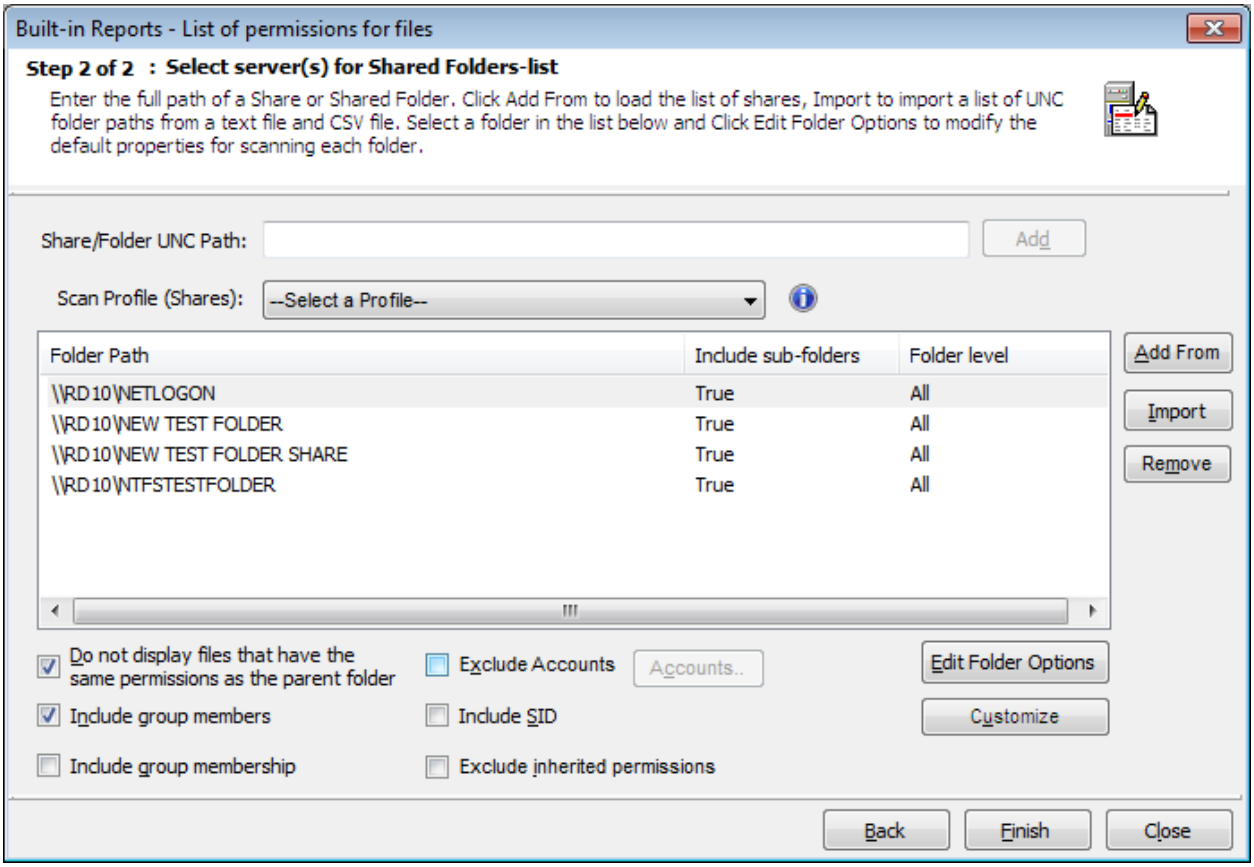

Built-in Reports - List of permissions for files
Step 1 of 2 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the permissions assigned to files under a specific folder.
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares


Built-in Reports - List of permissions for files
Step 2 of 2 : Select server
Enter the full path of a Share
folder paths from a text file.
properties for scanning each
Share/Folder UNC Path:
Scan Profile (Shares):
Folder Path
Add From
Import
Remove
Do not display files that ha
same permissions as the p
Include group members int
Include group membership
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Add Domains
Scan Profiles (Computers)
Sample Scans
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\TestShareFolder
OK
Cancel

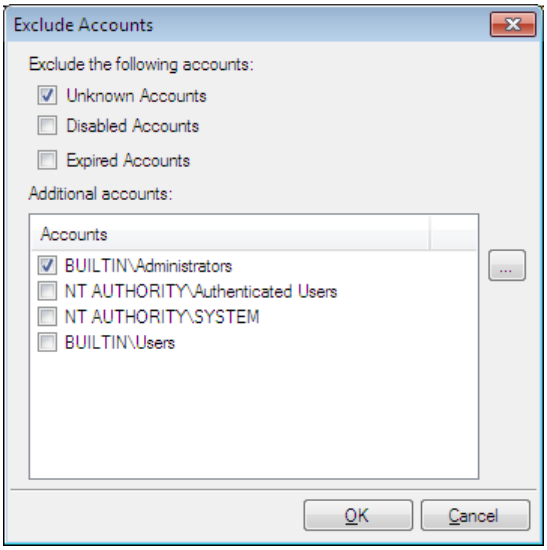


You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

If you want to exclude specific accounts from reporting, select **Exclude Accounts** option. Click **Accounts...** button to launch **Exclude Accounts** window, as shown below:



Select the accounts for which you want to exclude and click OK.

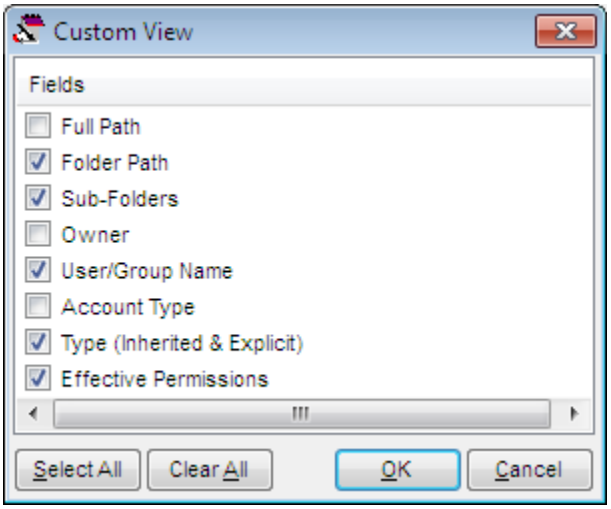
You can select **Include SID** option to include SID value for user in the report.

You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.

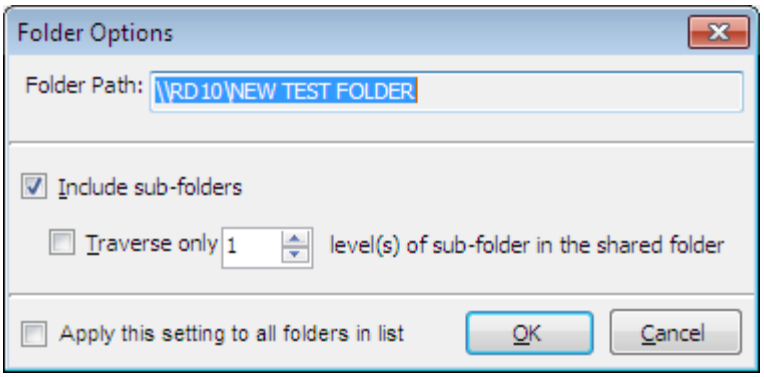
You can select **Include group membership** option to include all the membership information of user and group in the report.

You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



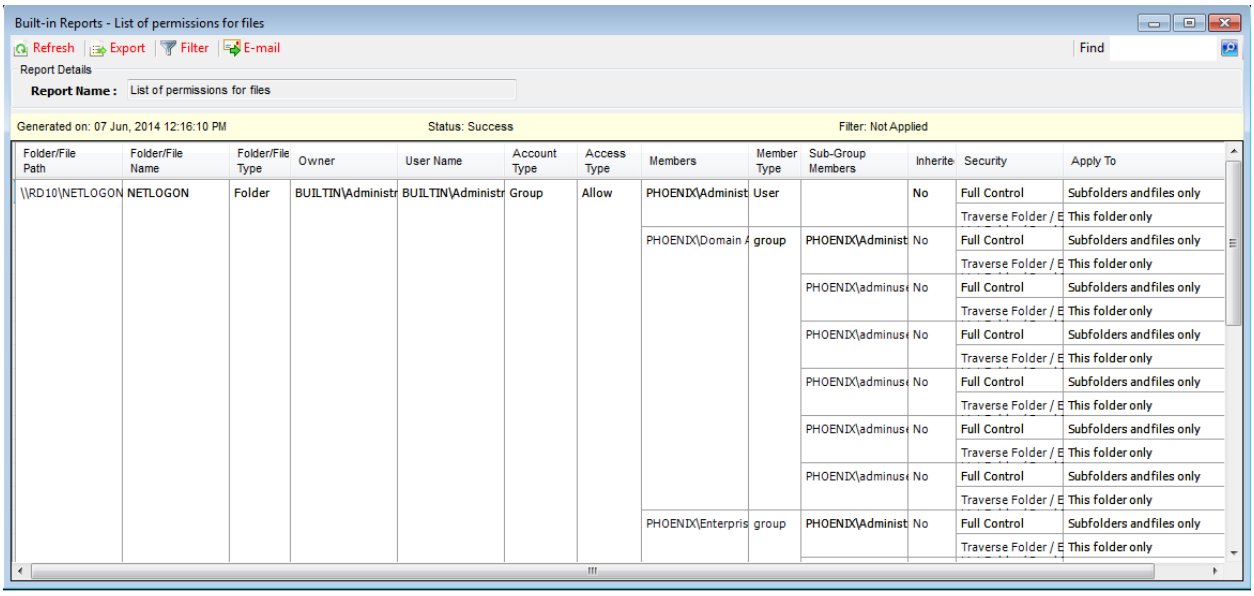
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

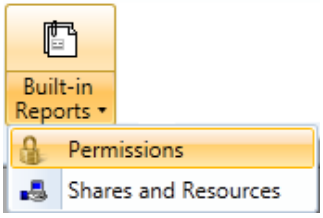
Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



List of all permissions for folders (Inherited & Explicit)

This report lists the permissions (explicit and inherit) assigned to the users for a set of folders.

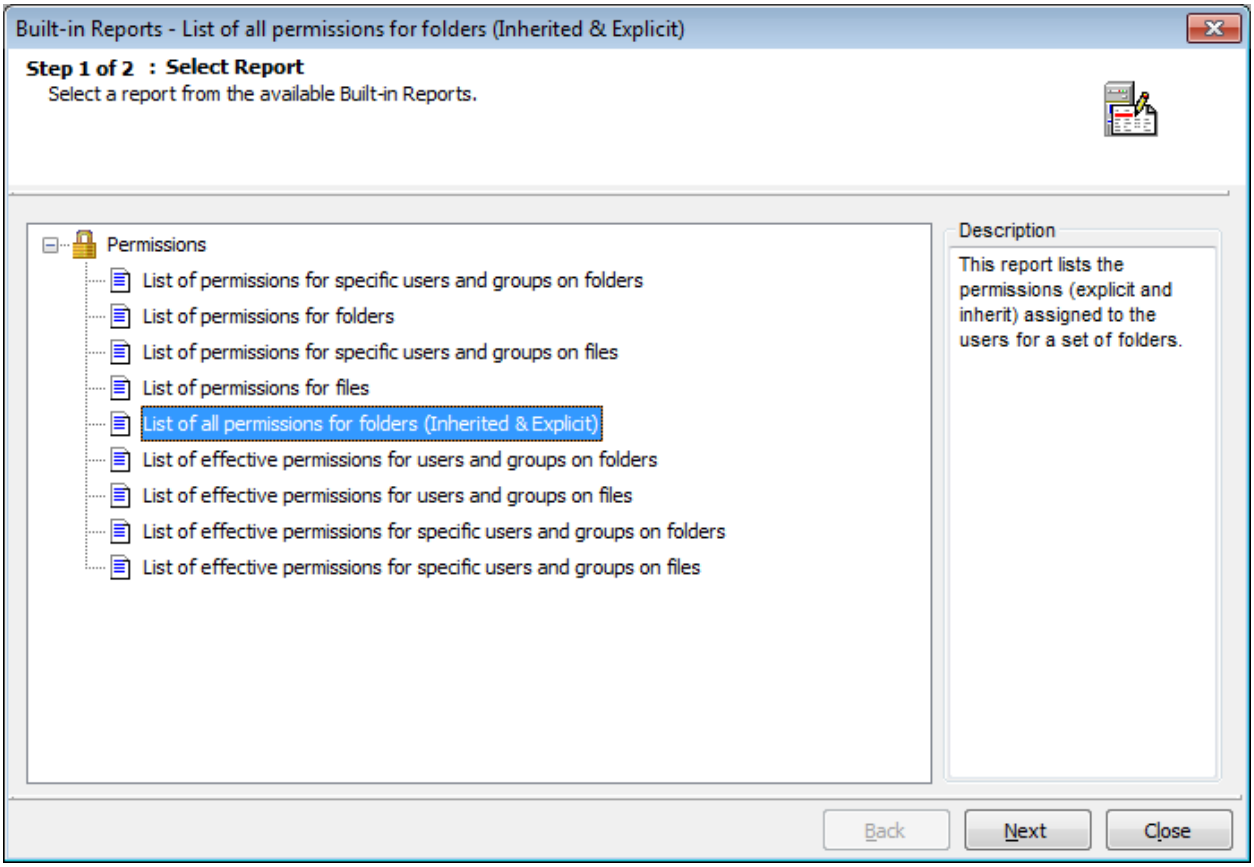
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

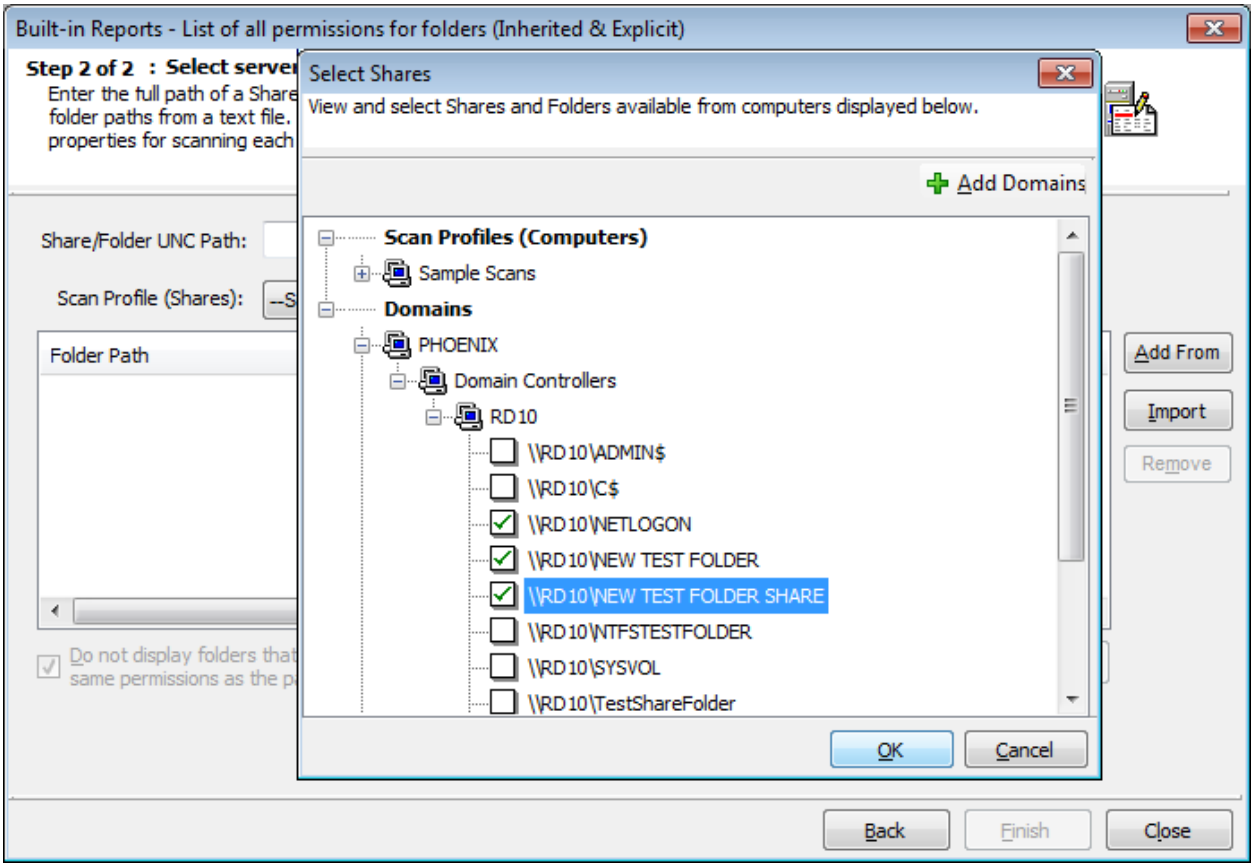
Select the report to be generated. Only one report can be generated at a time.

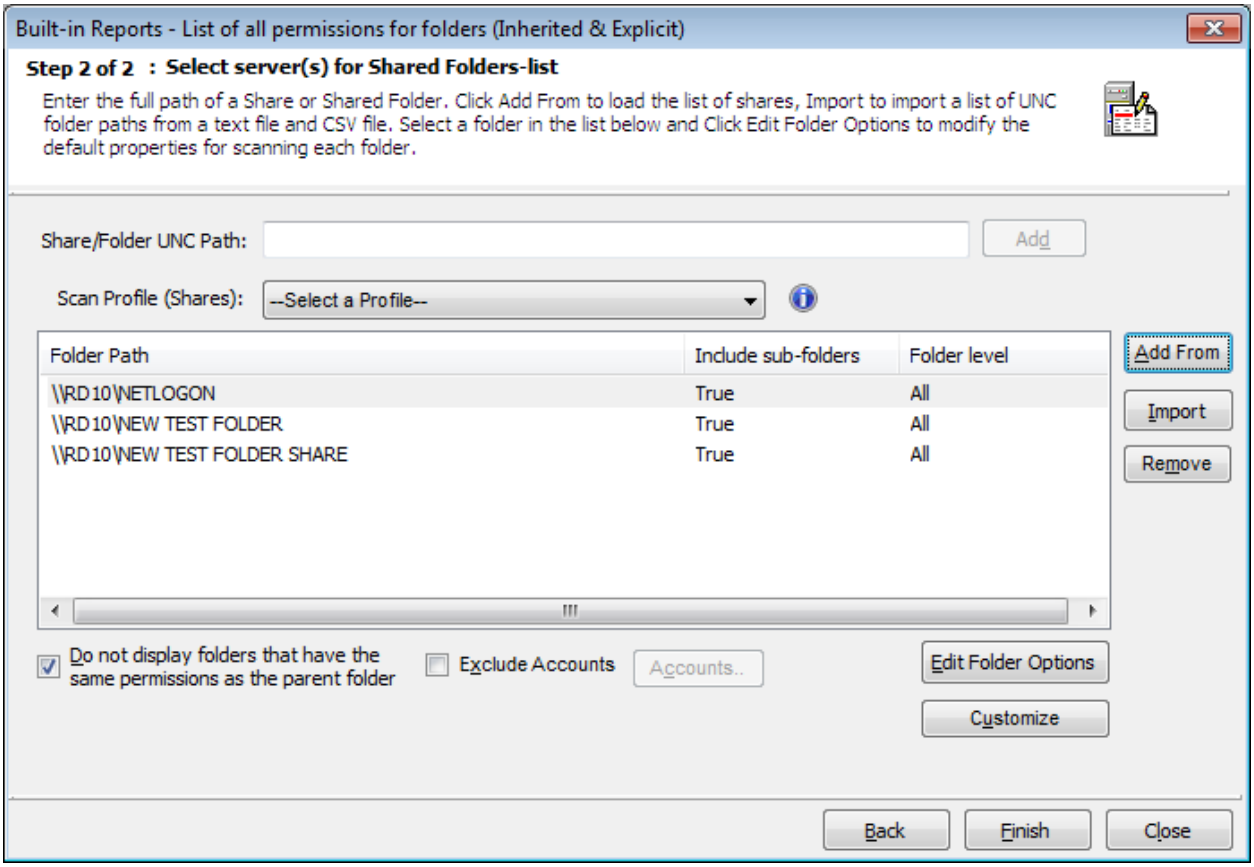

Built-in Reports - List of all permissions for folders (Inherited & Explicit)
Step 1 of 2 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the permissions (explicit and inherit) assigned to the users for a set of folders.
Back
Next
Close

Click Next to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares


Built-in Reports - List of all permissions for folders (Inherited & Explicit)
Step 2 of 2 : Select server
Enter the full path of a Share
folder paths from a text file.
properties for scanning each
Share/Folder UNC Path:
Scan Profile (Shares):
Folder Path
Do not display folders that
same permissions as the p
Add From
Import
Remove
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Add Domains
Scan Profiles (Computers)
Sample Scans
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\TestShareFolder
OK
Cancel

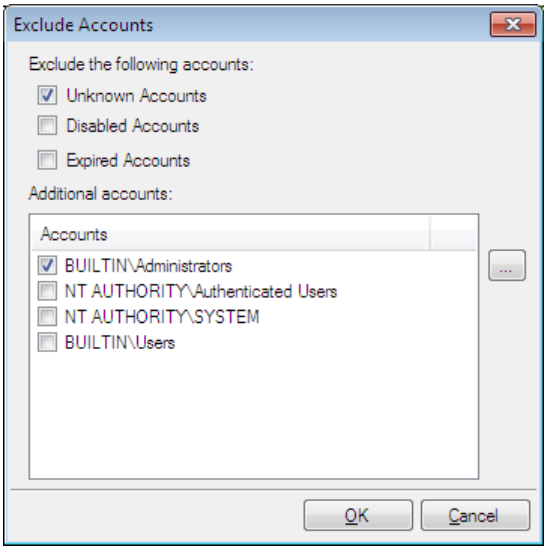

Built-in Reports - List of all permissions for folders (Inherited & Explicit)
Step 2 of 2 : Select server(s) for Shared Folders-list
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
Add From
Import
Remove
Do not display folders that have the same permissions as the parent folder
Exclude Accounts
Accounts..
Edit Folder Options
Customize
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

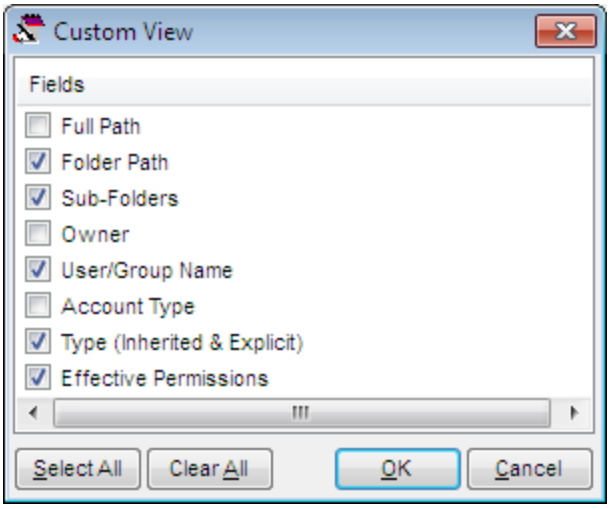
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

If you want to exclude specific accounts from reporting, select **Exclude Accounts** option. Click **Accounts...** button to launch **Exclude Accounts** window, as shown below:

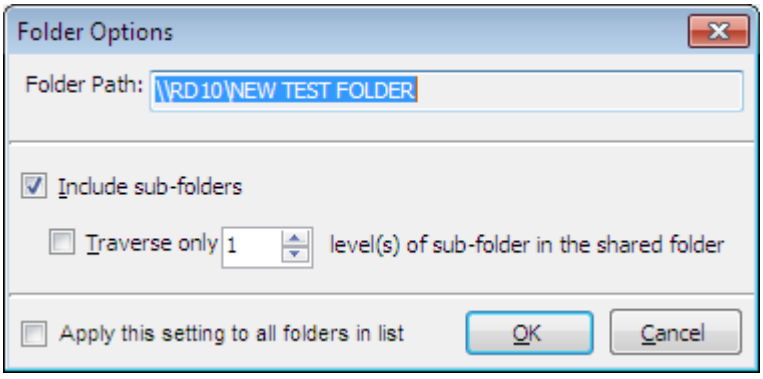


Select the accounts for which you want to exclude and click OK.

You can use Customize option to exclude some of the fields from the report, as displayed below:



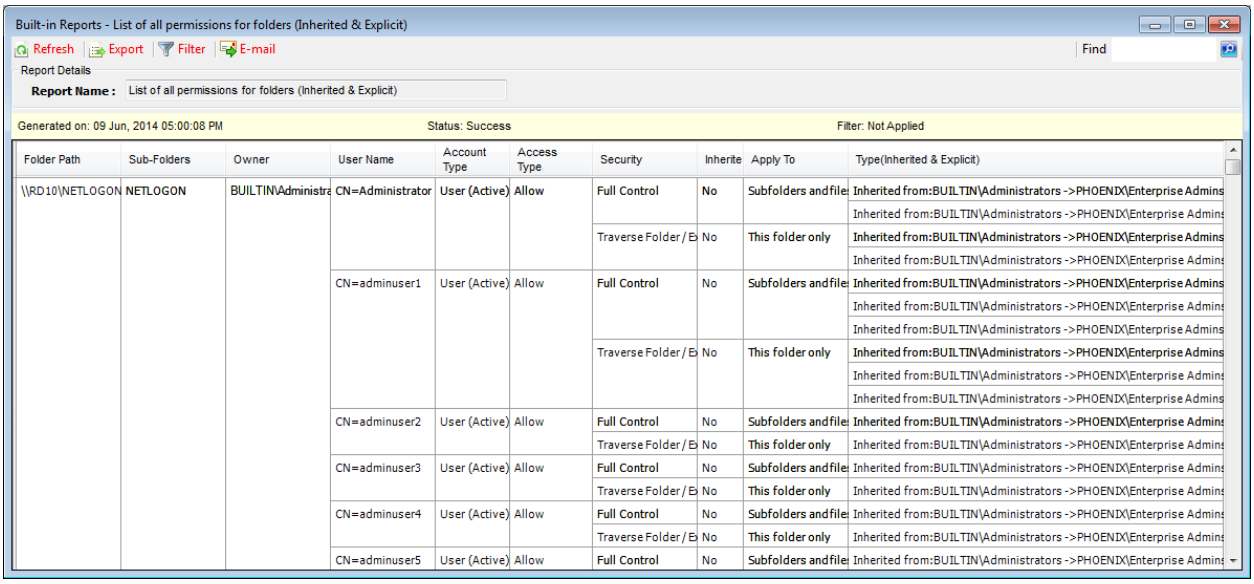
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

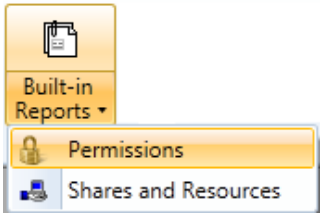
After the data collection process is complete, the report would be generated in a report window as shown below:



Folder Path	Sub-Folders	Owner	User Name	Account Type	Access Type	Security	Inherite	Apply To	Type(Inherited & Explicit)
\\RD10\NETLOGON	NETLOGON	BUILTIN\Administra	CN=Administrator	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
						Traverse Folder / E	No	This folder only	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
			CN=adminuser1	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
						Traverse Folder / E	No	This folder only	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
									Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
			CN=adminuser2	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
						Traverse Folder / E	No	This folder only	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
			CN=adminuser3	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
						Traverse Folder / E	No	This folder only	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
			CN=adminuser4	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
						Traverse Folder / E	No	This folder only	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins
			CN=adminuser5	User (Active)	Allow	Full Control	No	Subfolders andfile	Inherited from:BUILTIN\Administrators ->PHOENIX\Enterprise Admins

List of effective permission for users and groups on folders

This report lists the effective permissions for users and groups assigned to set of folders.

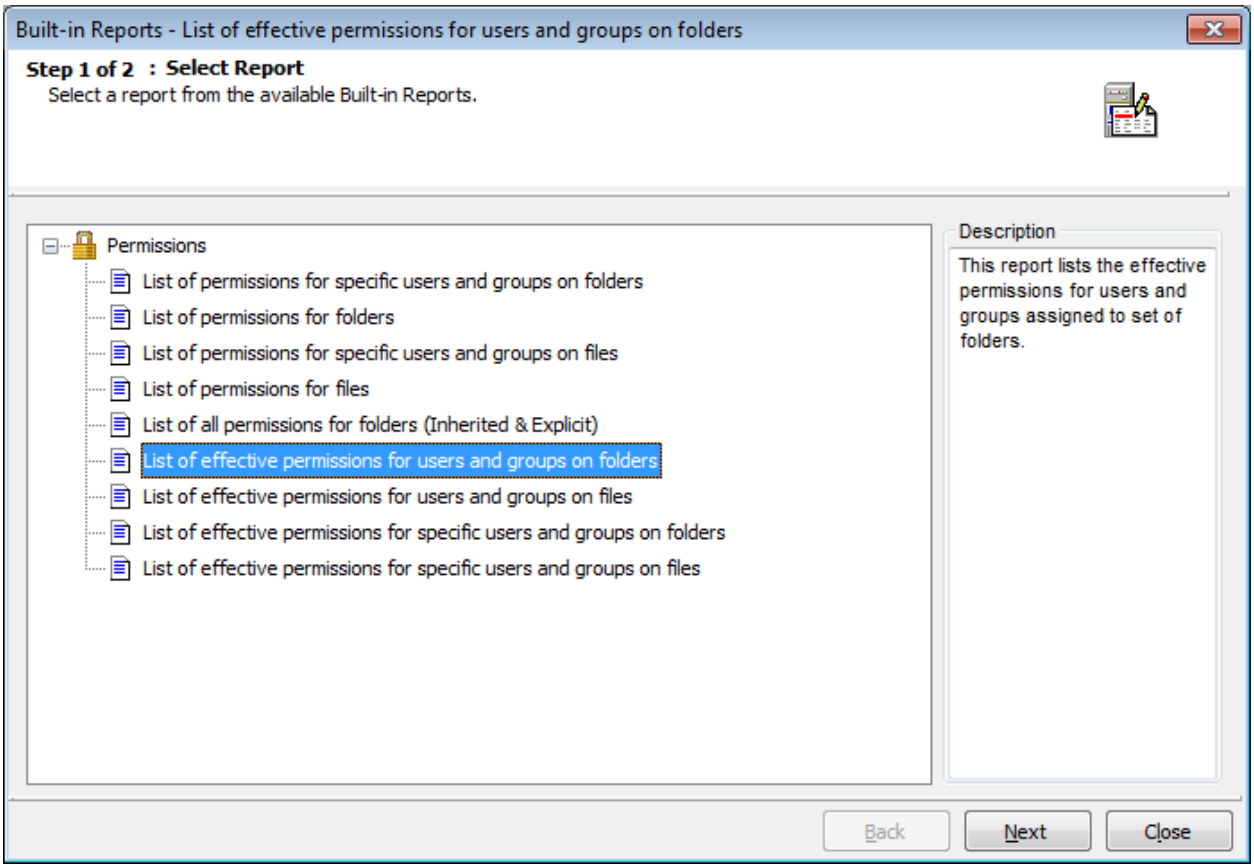
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

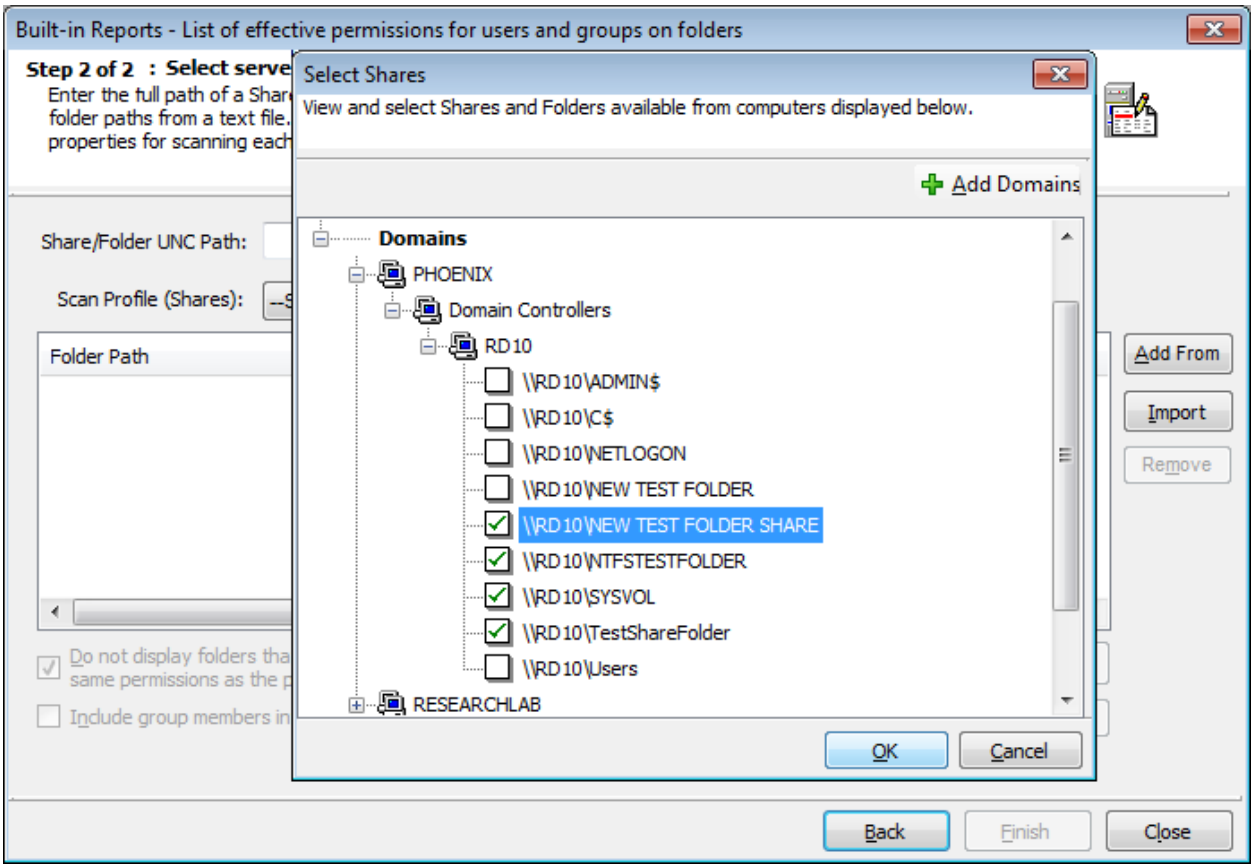
Select the report to be generated. Only one report can be generated at a time.

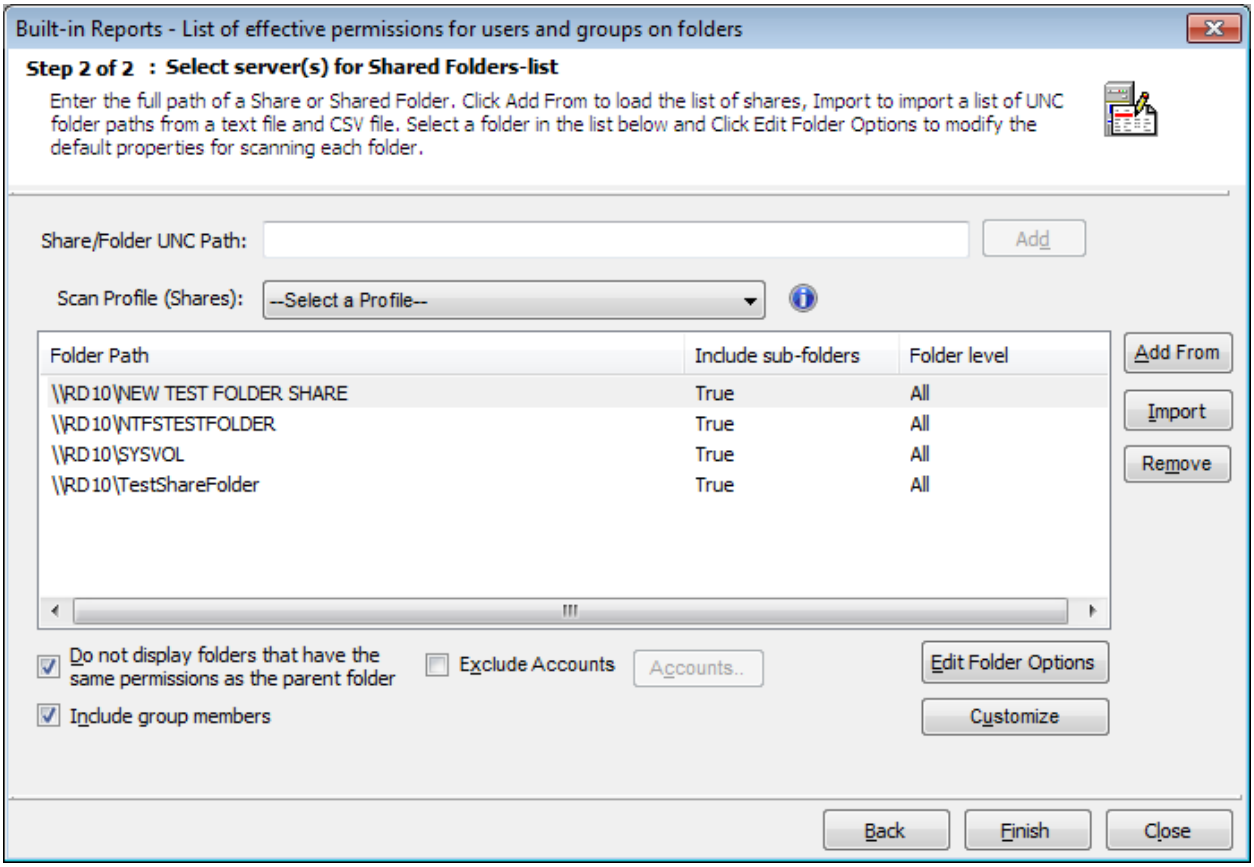

Built-in Reports - List of effective permissions for users and groups on folders
Step 1 of 2 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the effective permissions for users and groups assigned to set of folders.
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares



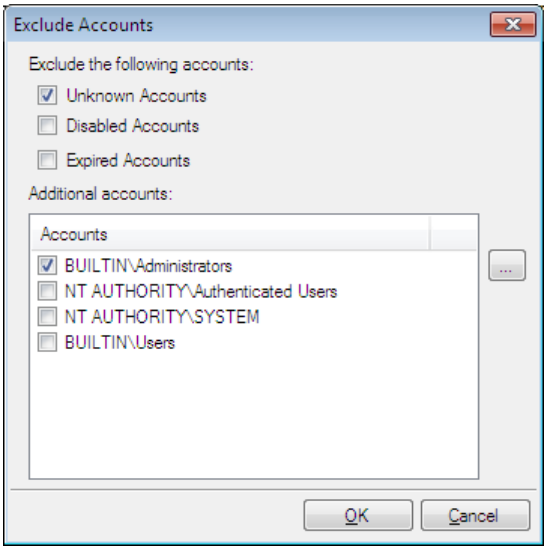

Built-in Reports - List of effective permissions for users and groups on folders
Step 2 of 2 : Select server(s) for Shared Folders-list
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\NTFSTESTFOLDER
True
All
\\RD10\SYSVOL
True
All
\\RD10\TestShareFolder
True
All
Add From
Import
Remove
Do not display folders that have the same permissions as the parent folder
Exclude Accounts
Accounts..
Edit Folder Options
Include group members
Customize
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

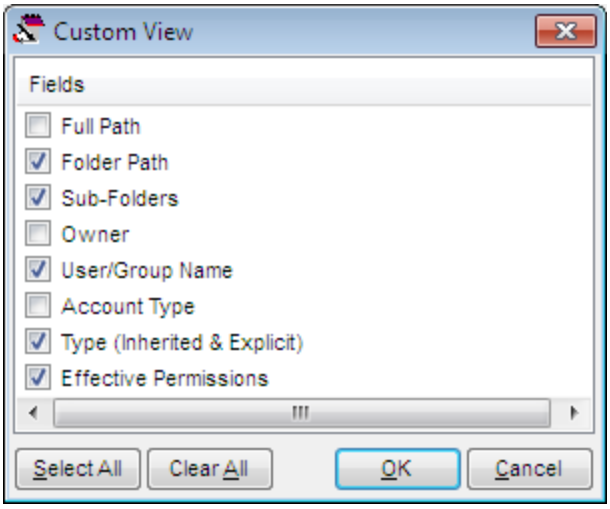
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

If you want to exclude specific accounts from reporting, select **Exclude Accounts** option. Click **Accounts...** button to launch **Exclude Accounts** window, as shown below:



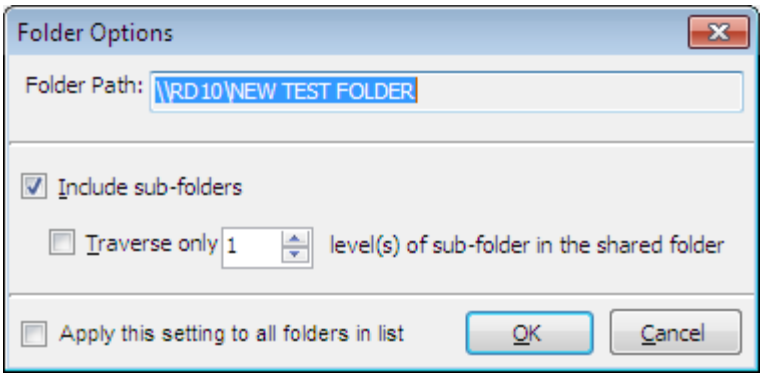
Select the accounts which you want to exclude and click **OK**.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

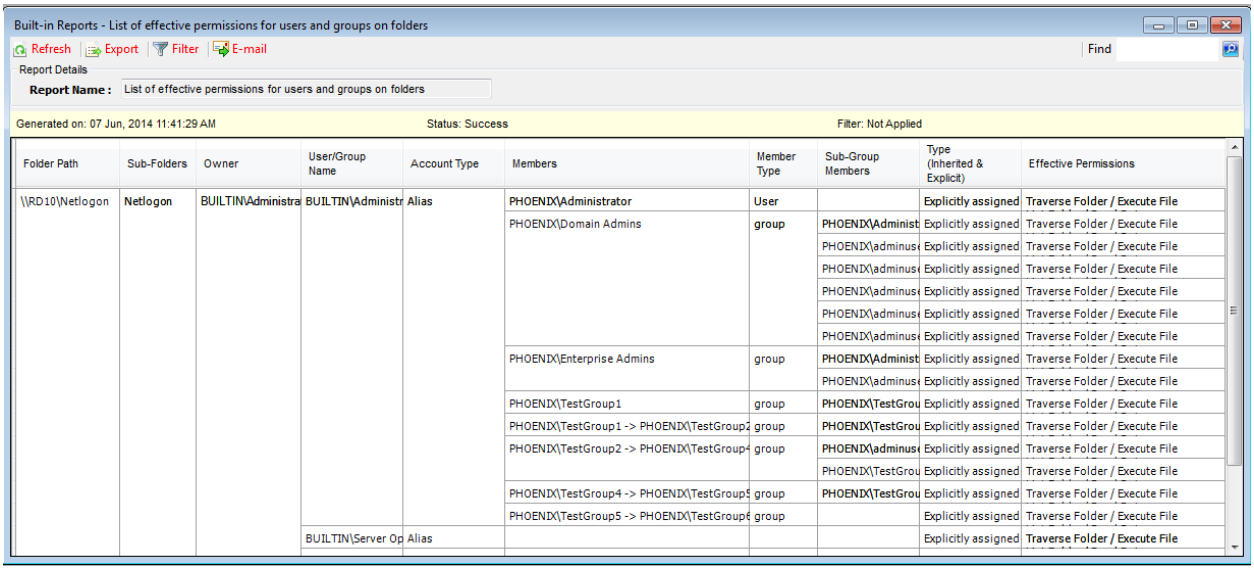
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.


Folder Options
Folder Path: \\RD10\NEW TEST FOLDER
Include sub-folders
Traverse only 1 level(s) of sub-folder in the shared folder
Apply this setting to all folders in list
OK
Cancel

Click **OK** to proceed.

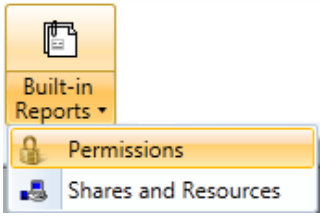
Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



List of effective permission for users and groups on files

This report lists the effective permissions for users and groups assigned to files available in a set of folders.

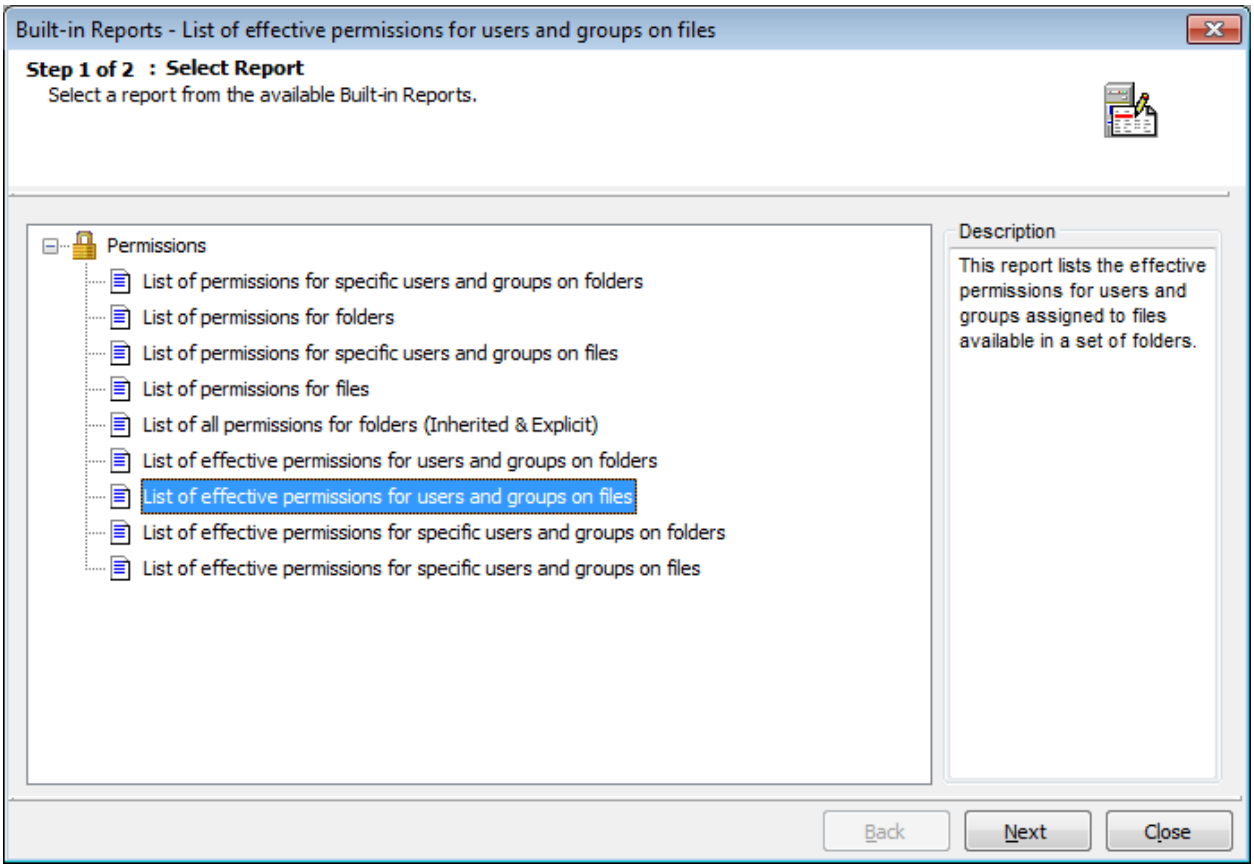
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

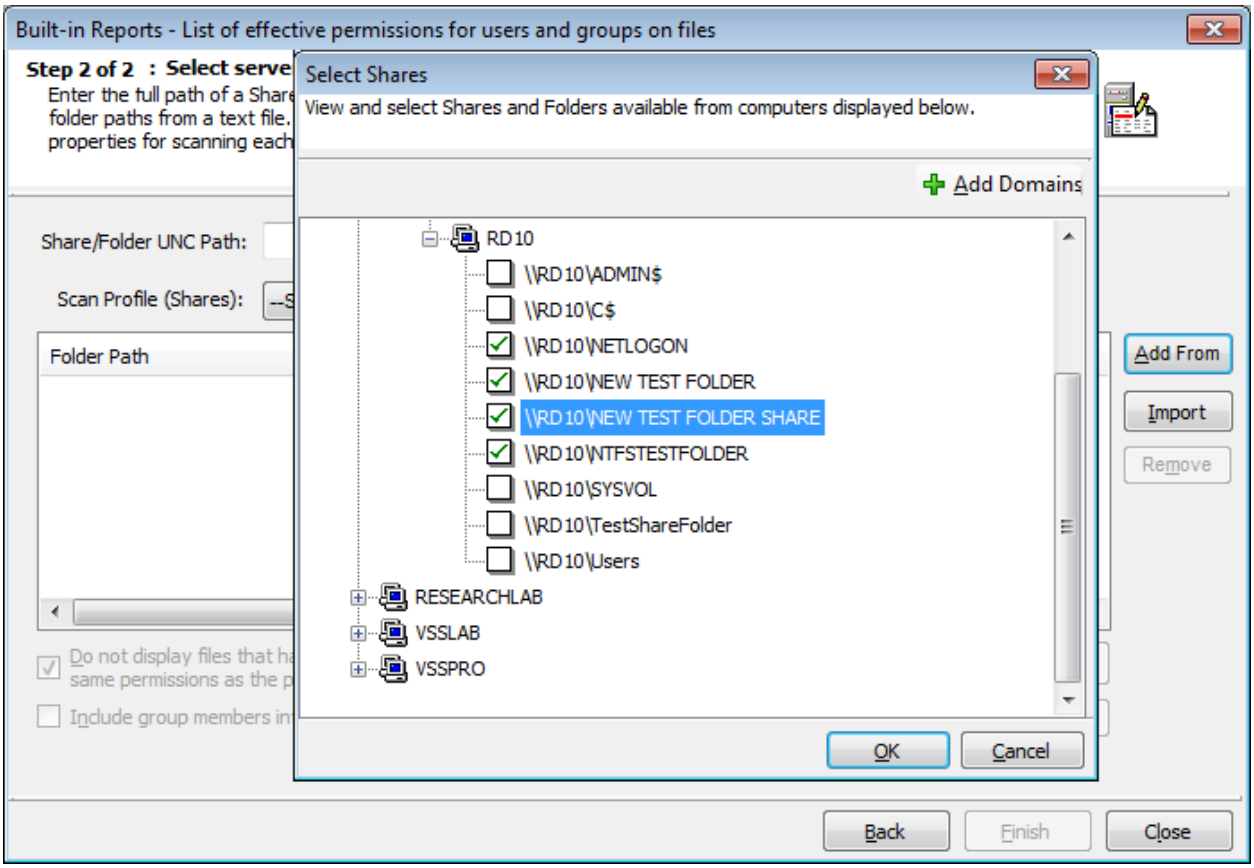
Select the report to be generated. Only one report can be generated at a time.

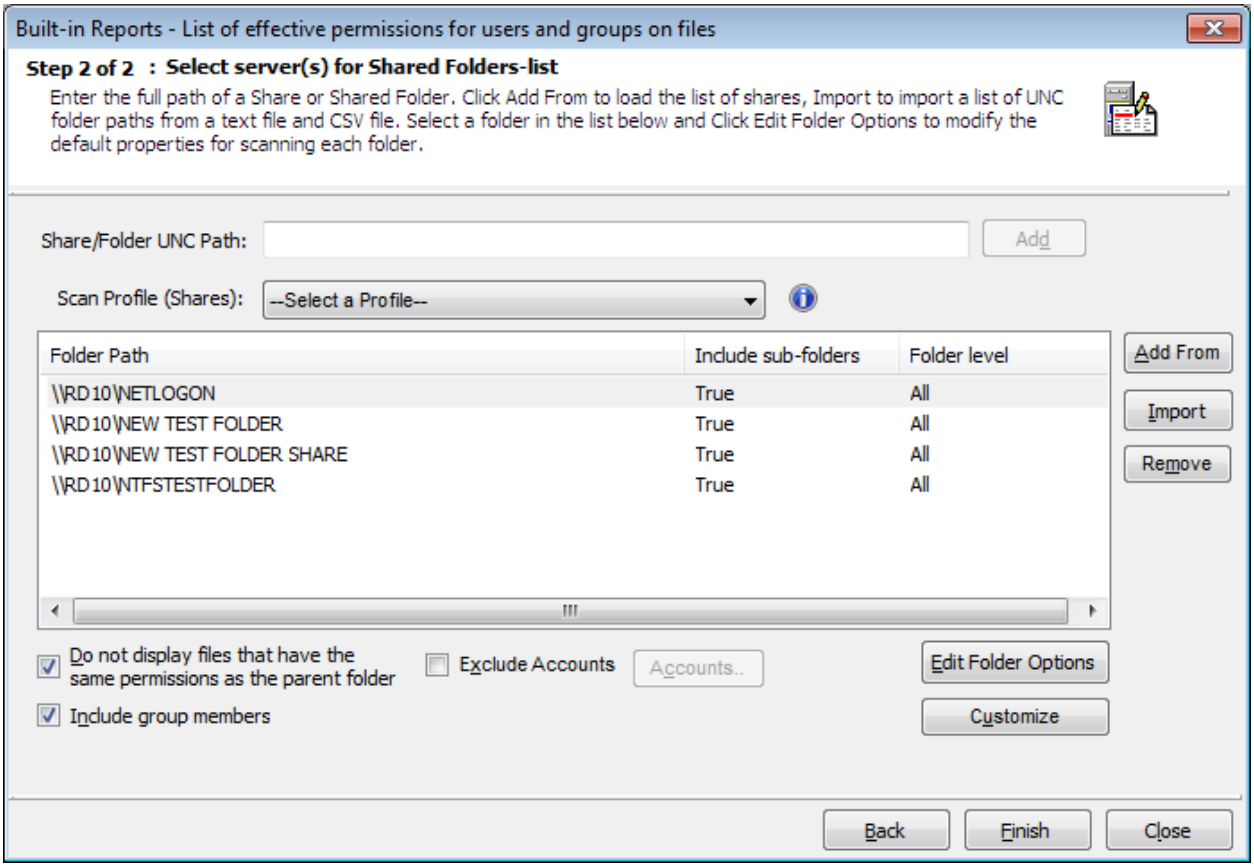

Built-in Reports - List of effective permissions for users and groups on files
Step 1 of 2 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the effective permissions for users and groups assigned to files available in a set of folders.
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares



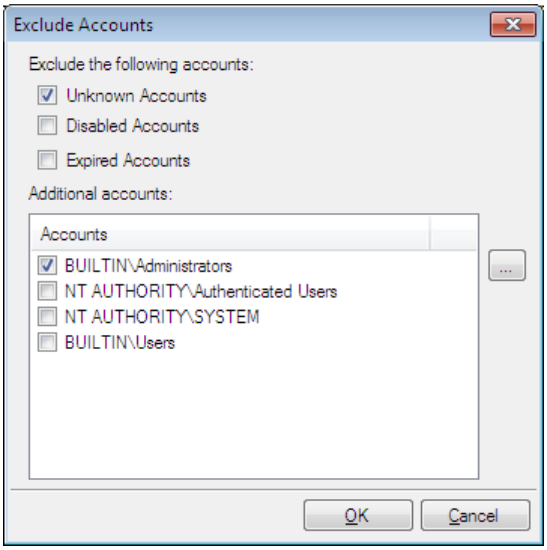

Built-in Reports - List of effective permissions for users and groups on files
Step 2 of 2 : Select server(s) for Shared Folders-list
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\NTFSTESTFOLDER
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Exclude Accounts
Accounts..
Edit Folder Options
Include group members
Customize
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

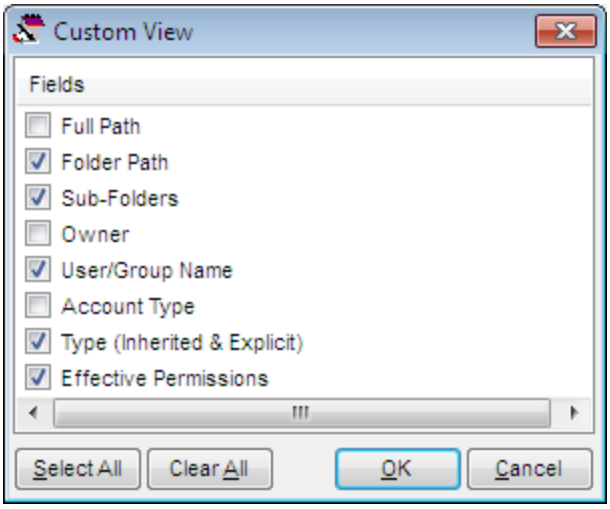
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

If you want to exclude specific accounts from reporting, select **Exclude Accounts** option. Click **Accounts...** button to launch **Exclude Accounts** window, as shown below:



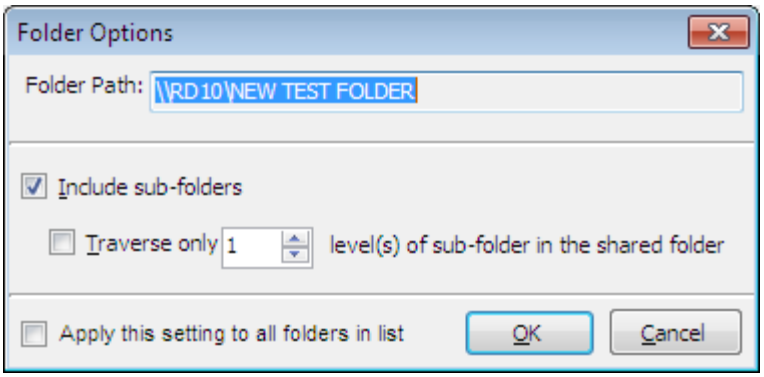
Select the accounts which you want to exclude and click OK.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



You can select **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

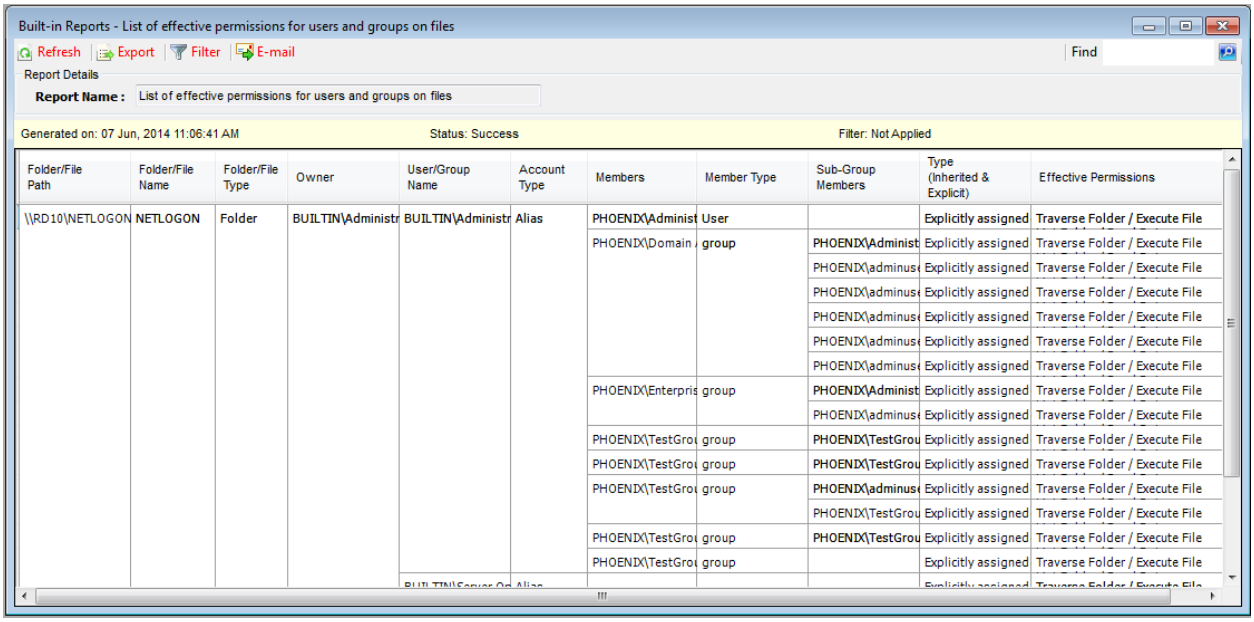
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

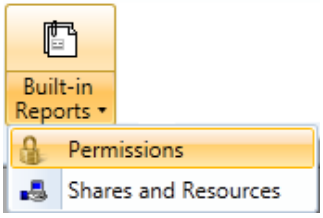
Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



List of effective permissions for specific users and groups on folders

This report lists the effective permissions assigned to a specific user/group account for a set of folders.

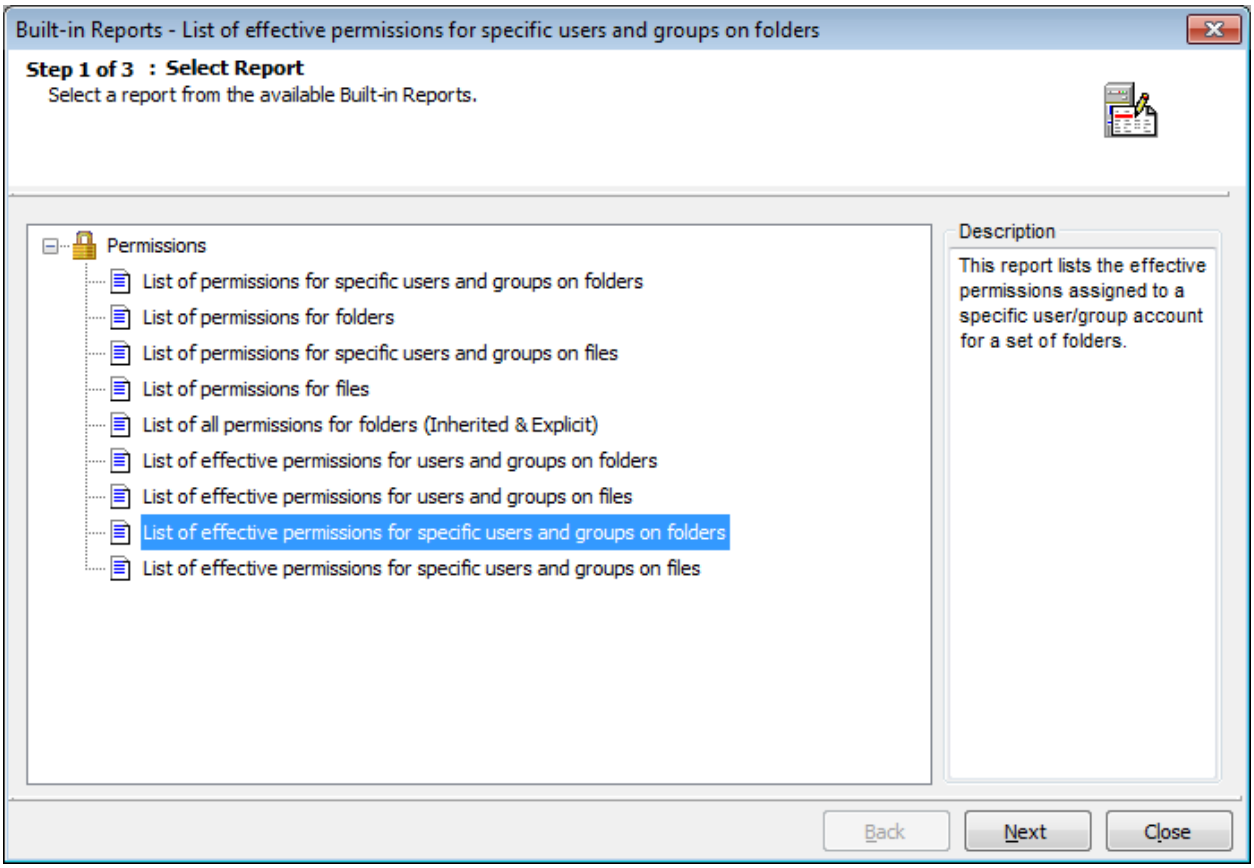
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

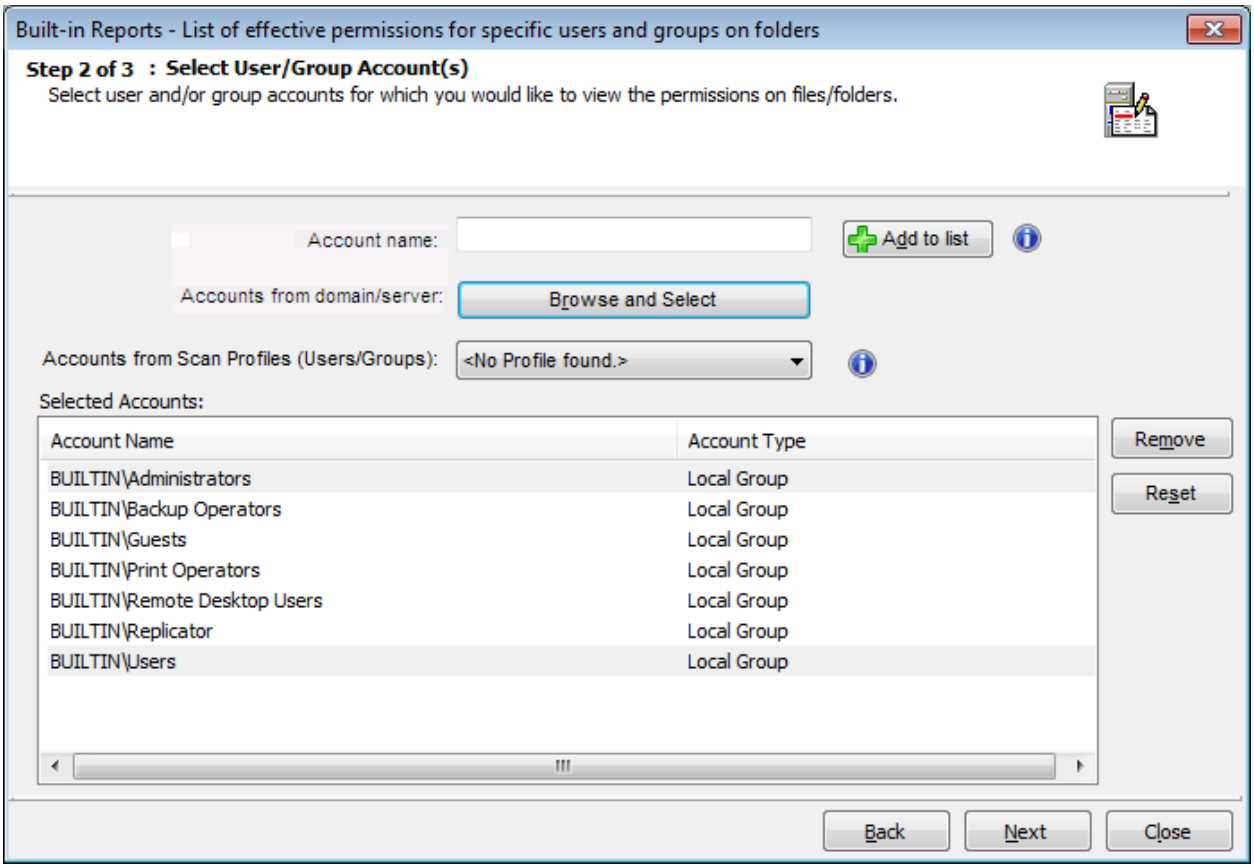
Select the report to be generated. Only one report can be generated at a time.


Built-in Reports - List of effective permissions for specific users and groups on folders
Step 1 of 3 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the effective permissions assigned to a specific user/group account for a set of folders.
Back
Next
Close

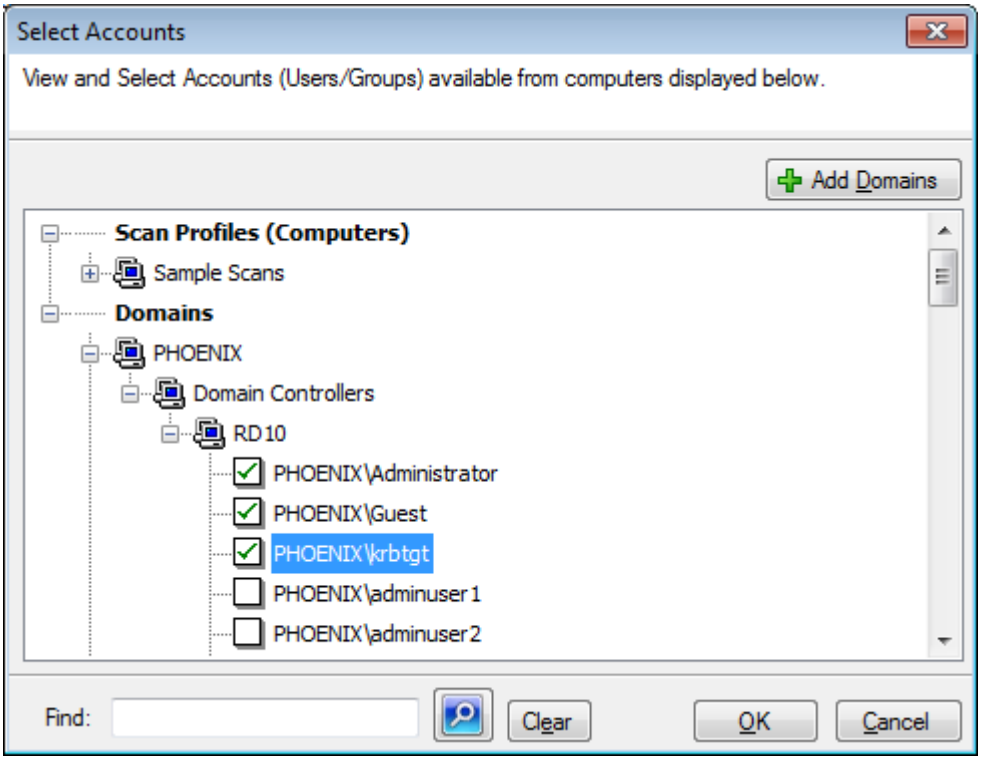
Click **Next** to proceed to the next step.

Step 2: Select User/Group Accounts

Select user and/or group accounts for which you would like to view the permissions for folders/files.



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list
- Use Select a **Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).

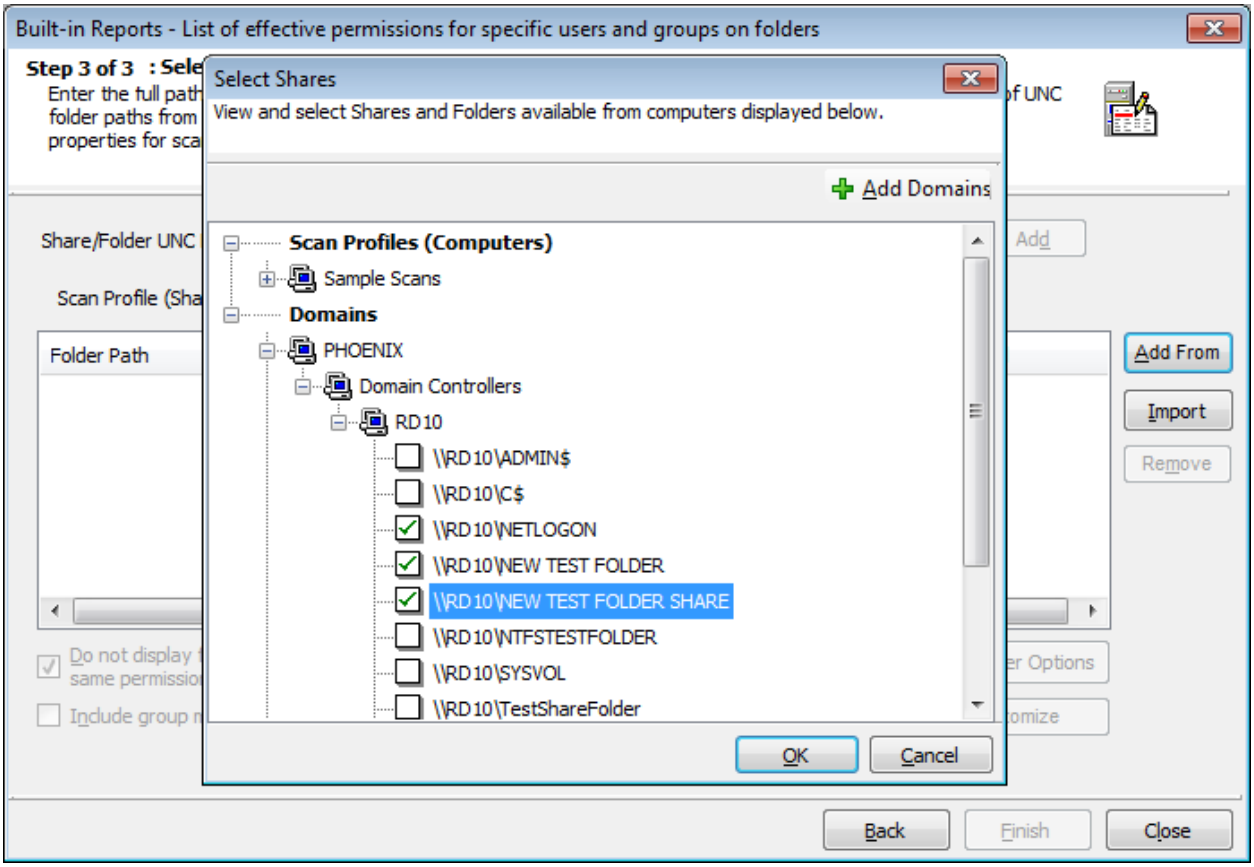


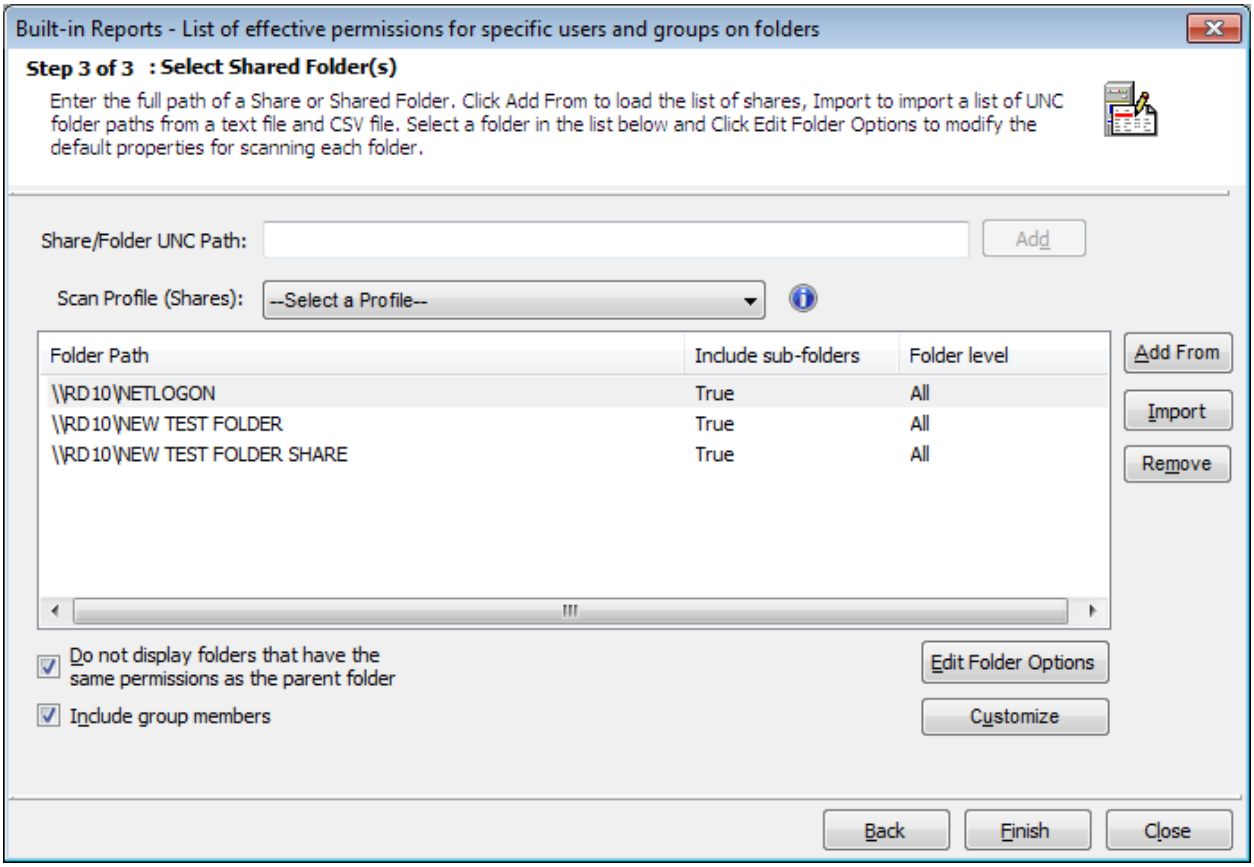
- Use the **Find** option to search desired user/group accounts.

Click **Next** to proceed.

Step 3: Select shared folders

Select one or more servers to retrieve available shares.


Built-in Reports - List of effective permissions for specific users and groups on folders
Step 3 of 3 : Sele
Enter the full path
folder paths from
properties for sca
Share/Folder UNC
Scan Profile (Sha
Folder Path
Add From
Import
Remove
Add
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Add Domains
Scan Profiles (Computers)
Sample Scans
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\TestShareFolder
OK
Cancel

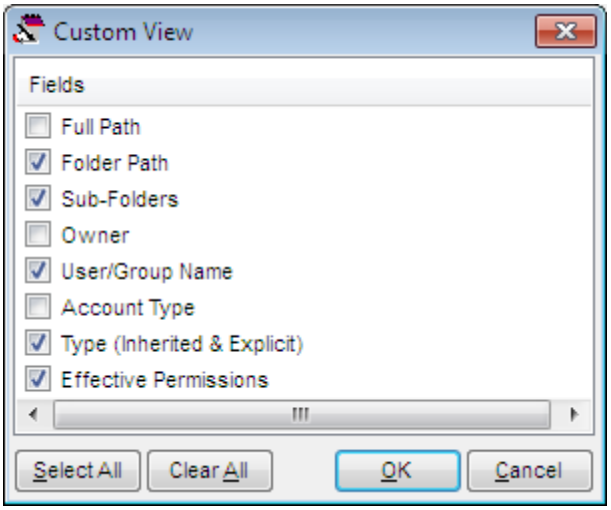

Built-in Reports - List of effective permissions for specific users and groups on folders
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
Add From
Import
Remove
Do not display folders that have the same permissions as the parent folder
Include group members
Edit Folder Options
Customize
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

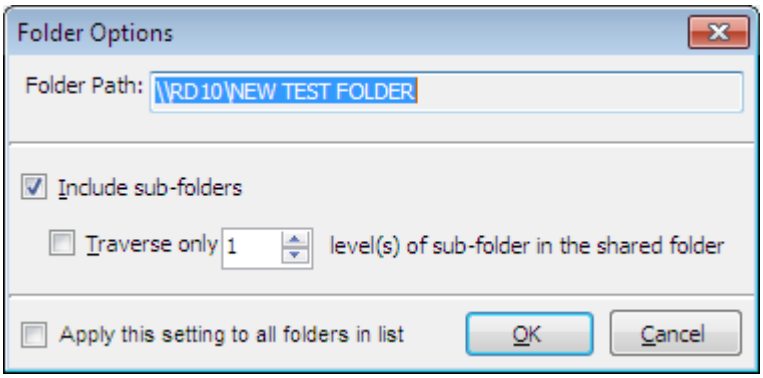
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



You can use **Include group members information** option to include all the members of a group and their sub-group members at all group levels in the report.

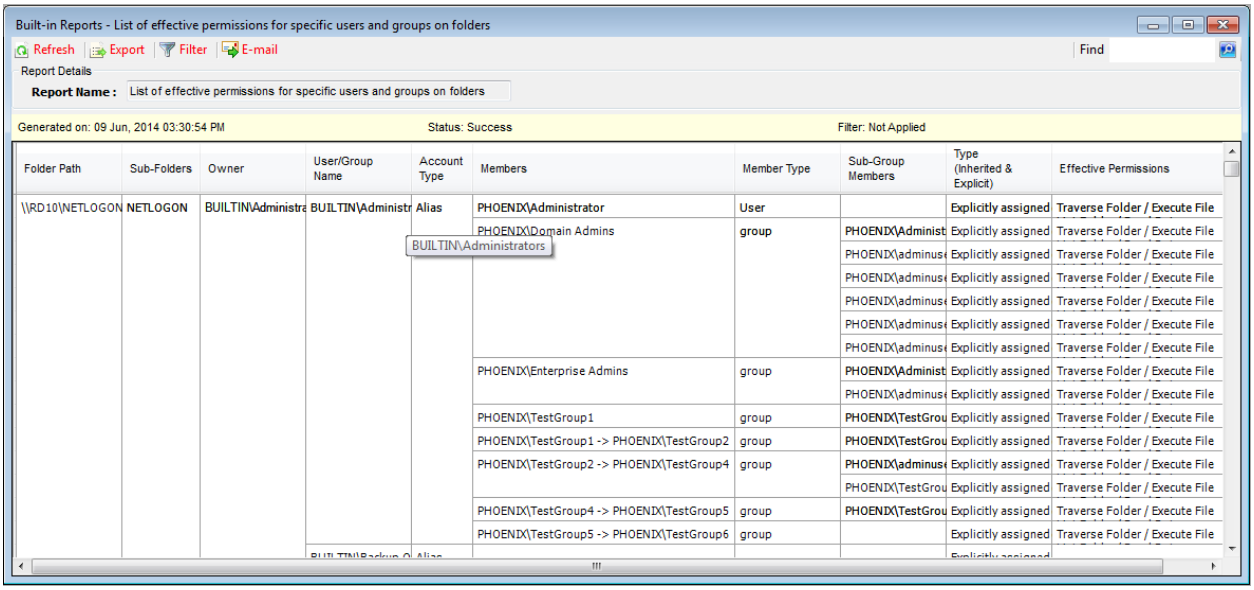
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

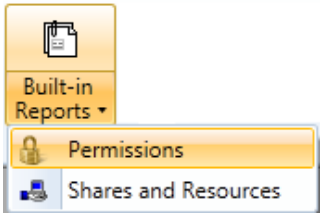
Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:


Built-in Reports - List of effective permissions for specific users and groups on folders
Refresh
Export
Filter
E-mail
Find
Report Details
Report Name : List of effective permissions for specific users and groups on folders
Generated on: 09 Jun, 2014 03:30:54 PM
Status: Success
Filter: Not Applied
Folder Path
Sub-Folders
Owner
User/Group Name
Account Type
Members
Member Type
Sub-Group Members
Type (Inherited & Explicit)
Effective Permissions
\\RD10\NETLOGON
NETLOGON
BUILTIN\Administra
BUILTIN\Administr
Alias
PHOENIX\Administrator
User
Explicitly assigned
Traverse Folder / Execute File
PHOENIX\Domain Admins
group
PHOENIX\Enterprise Admins
group
PHOENIX\TestGroup1
group
PHOENIX\TestGroup1 -> PHOENIX\TestGroup2
group
PHOENIX\TestGroup2 -> PHOENIX\TestGroup4
group
PHOENIX\TestGroup4 -> PHOENIX\TestGroup5
group
PHOENIX\TestGroup5 -> PHOENIX\TestGroup6
group
BUILTIN\Administrators

List of effective permissions for specific users and groups on files

This report lists the effective permissions assigned to a specific user/group account for files available in a set of folders.

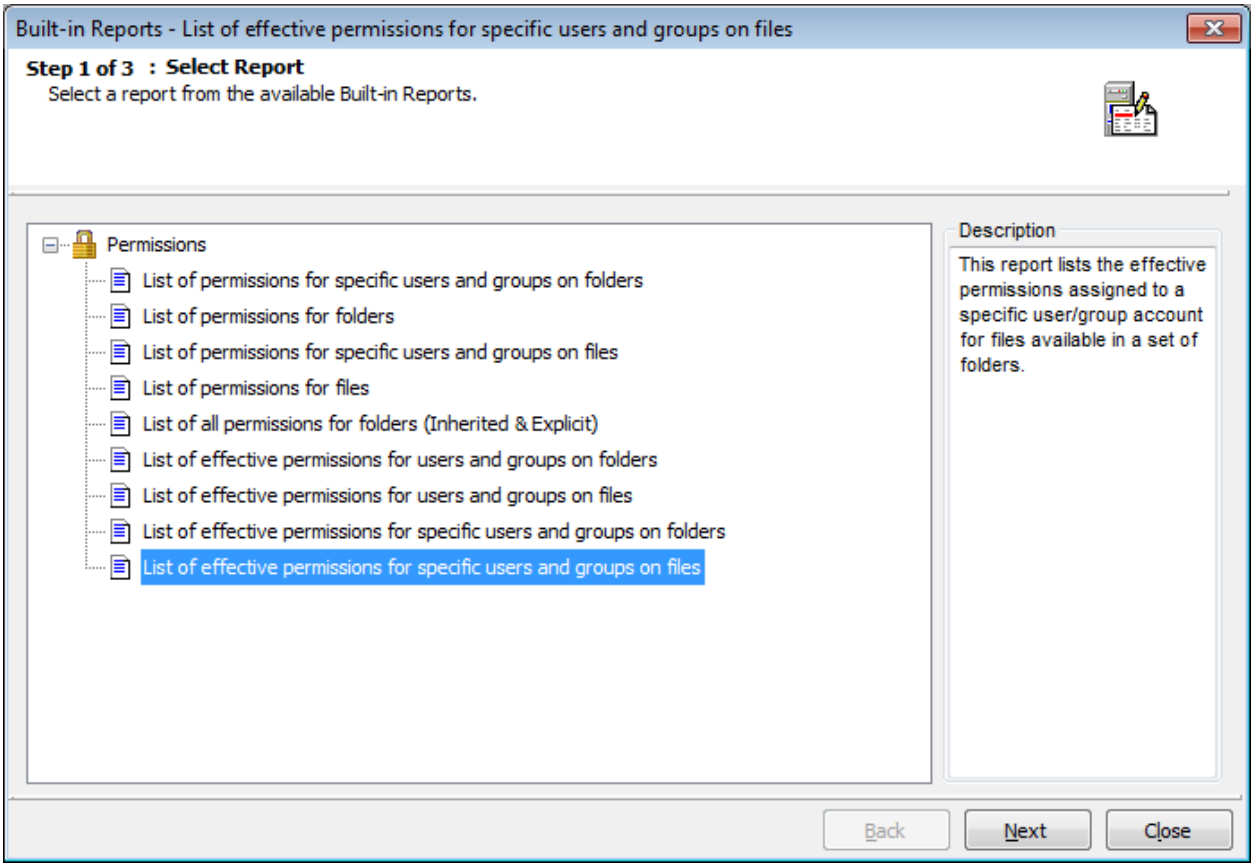
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

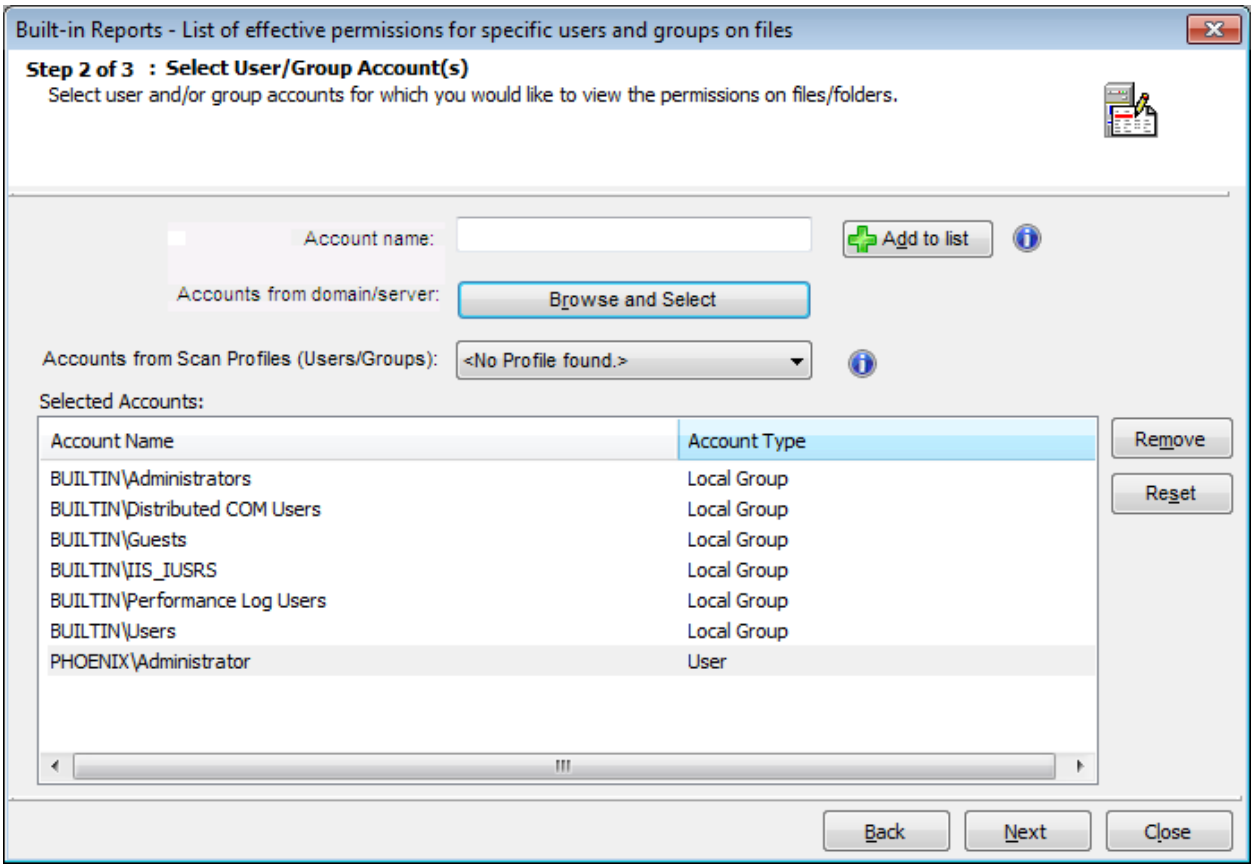
Select the report to be generated. Only one report can be generated at a time.


Built-in Reports - List of effective permissions for specific users and groups on files
Step 1 of 3 : Select Report
Select a report from the available Built-in Reports.
Permissions
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
Description
This report lists the effective permissions assigned to a specific user/group account for files available in a set of folders.
Back
Next
Close

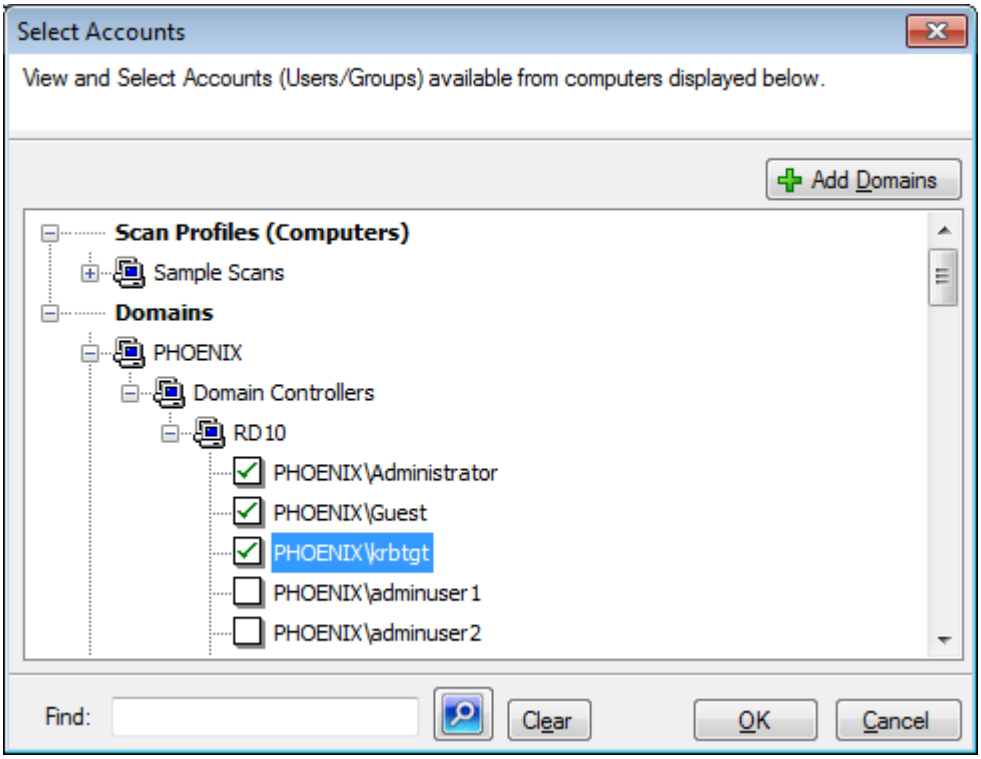
Click **Next** to proceed to the next step.

Step 2: Select User/Group Accounts

Select user and/or group accounts for which you would like to view the permissions for folders/files.



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).

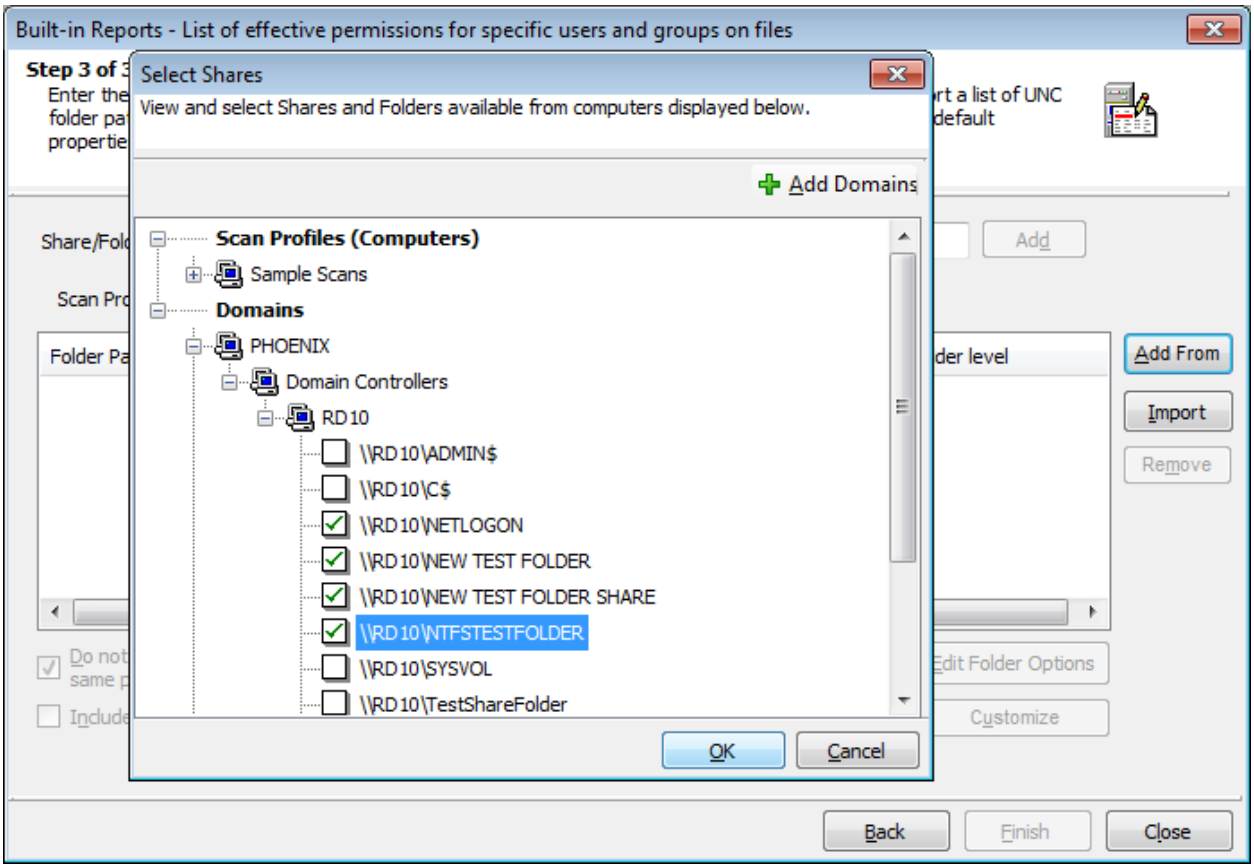


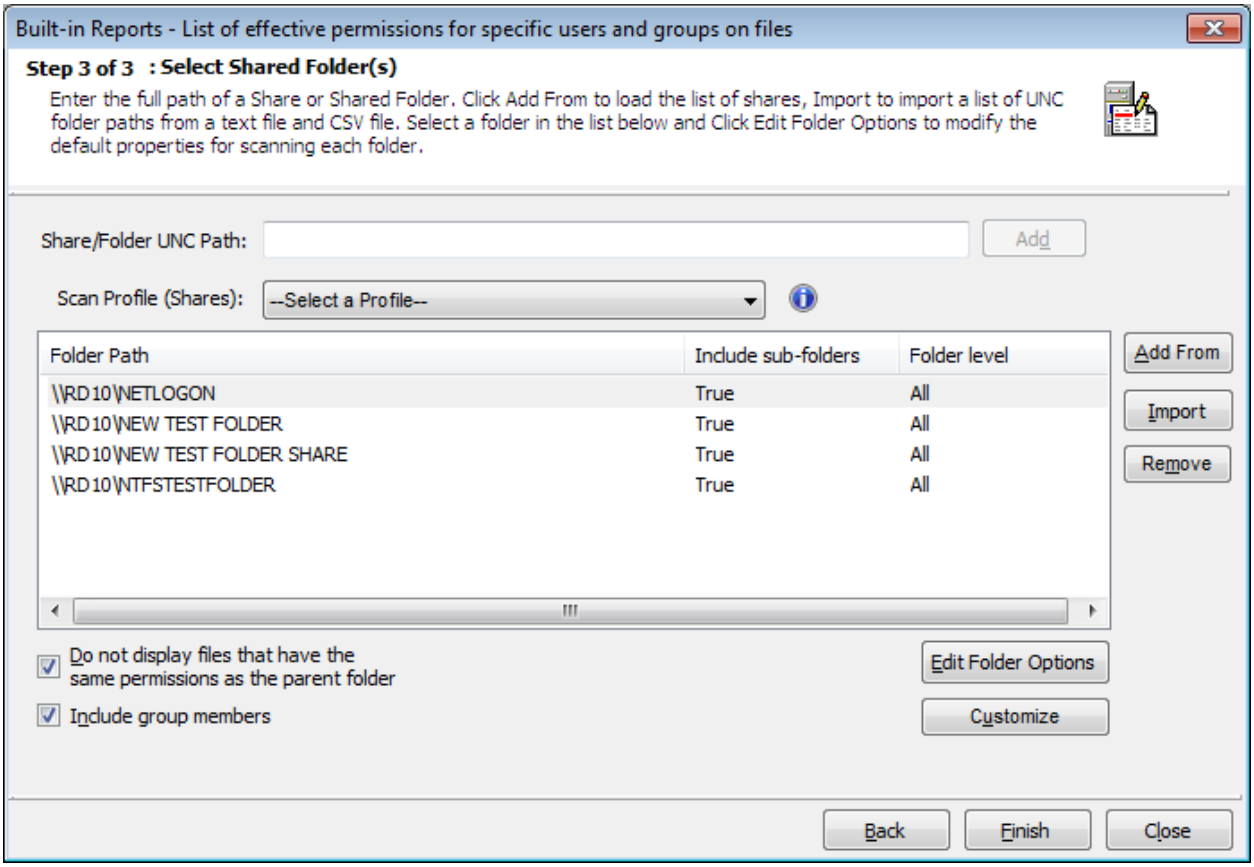
- Use the **Find** option to search desired user/group accounts.

Click **Next** to proceed.

Step 3: Select shared folders

Select one or more servers to retrieve available shares.



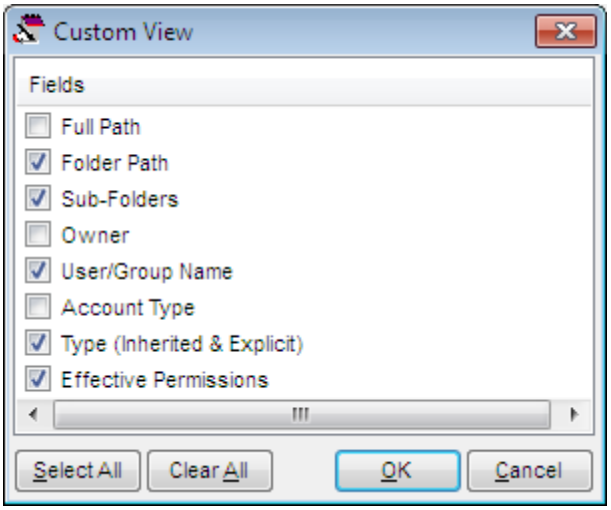

Built-in Reports - List of effective permissions for specific users and groups on files
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\NTFSTESTFOLDER
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include group members
Edit Folder Options
Customize
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

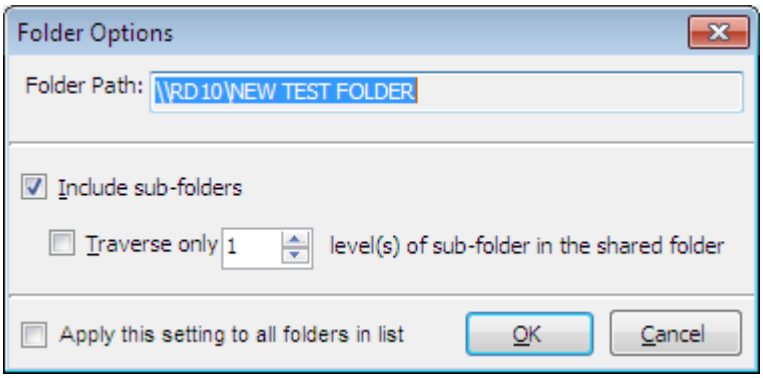
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

You can use **Customize** option to exclude some of the fields from the report, as displayed below:



You can use **Include group members** option to include all the members of a group and their sub-group members at all group levels in the report.

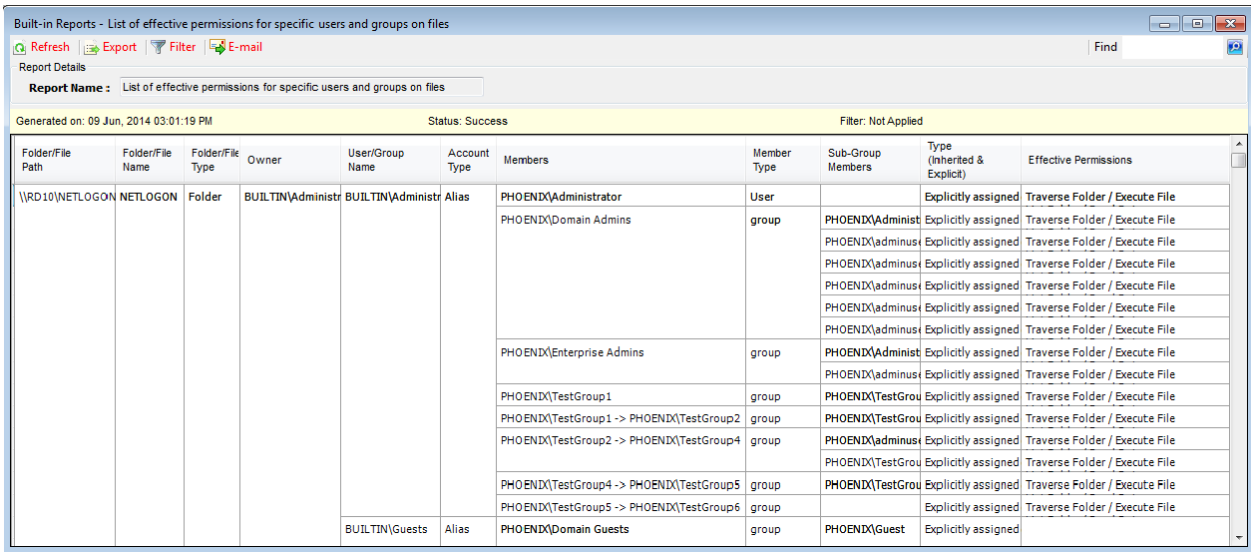
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



Built-in Reports - List of effective permissions for specific users and groups on files

Refresh | Export | Filter | E-mail | Find

Report Details

Report Name : List of effective permissions for specific users and groups on files

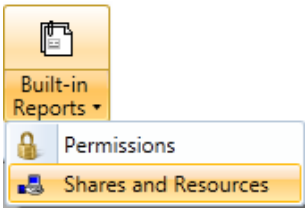
Generated on: 09 Jun, 2014 03:01:19 PM | Status: Success | Filter: Not Applied

Folder/File Path	Folder/File Name	Folder/File Type	Owner	User/Group Name	Account Type	Members	Member Type	Sub-Group Members	Type (Inherited & Explicit)	Effective Permissions
\\RD10\NETLOGON	NETLOGON	Folder	BUILTIN\Administr	BUILTIN\Administr	Alias	PHOENIX\Administrator	User		Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\Domain Admins	group	PHOENIX\Administ	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\Enterprise Admins	group	PHOENIX\Administ	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\TestGroup1	group	PHOENIX\TestGrou	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\TestGroup1 -> PHOENIX\TestGroup2	group	PHOENIX\TestGrou	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\TestGroup2 -> PHOENIX\TestGroup4	group	PHOENIX\adminus	Explicitly assigned	Traverse Folder / Execute File
								PHOENIX\TestGrou	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\TestGroup4 -> PHOENIX\TestGroup5	group	PHOENIX\TestGrou	Explicitly assigned	Traverse Folder / Execute File
						PHOENIX\TestGroup5 -> PHOENIX\TestGroup6	group		Explicitly assigned	Traverse Folder / Execute File
				BUILTIN\Guests	Alias	PHOENIX\Domain Guests	group	PHOENIX\Guest	Explicitly assigned	

How to view Built-in Reports for Shares and Resources?

Shares and Resources Reports

The Shares and Resources reports can be generated against domains(s) and specific sever(s) as well.

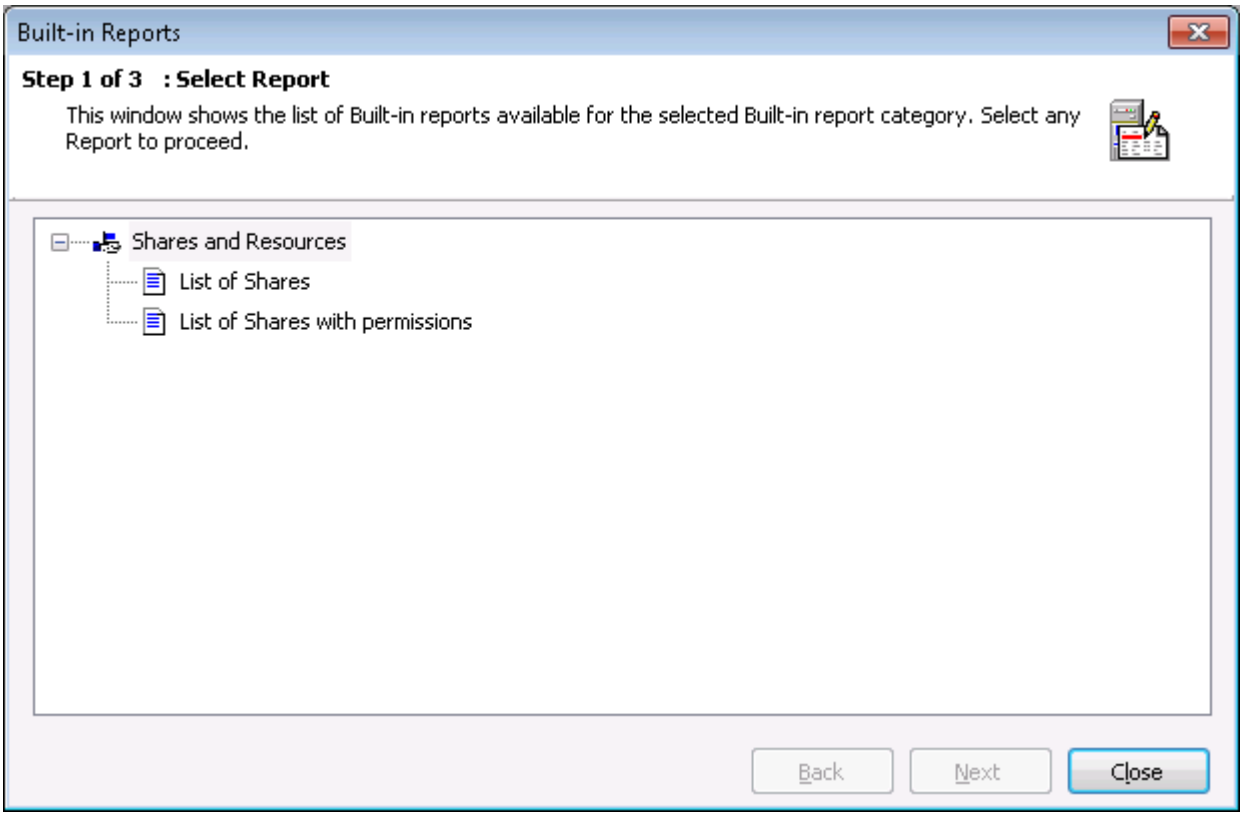
Click on 

button under Built-in Reports.

The Built-in Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

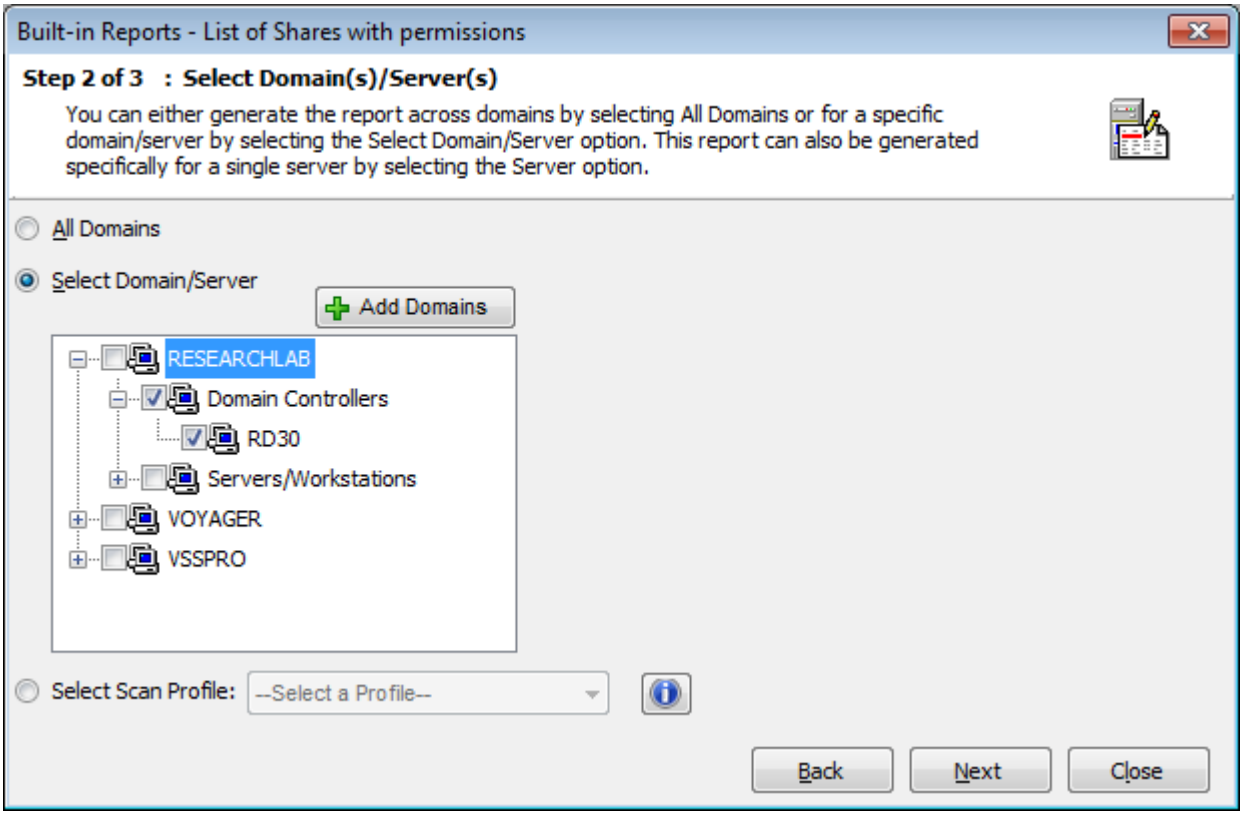
Select the report to be generated. Only one report can be generated at a time. Click Next to proceed to the next step.


Built-in Reports
Step 1 of 3 : Select Report
This window shows the list of Built-in reports available for the selected Built-in report category. Select any Report to proceed.
Shares and Resources
List of Shares
List of Shares with permissions
Back
Next
Close

Step 2: Select Domain(s) / Server(s)

Select the server(s) / Domain(s), for which the report needs to be generated.

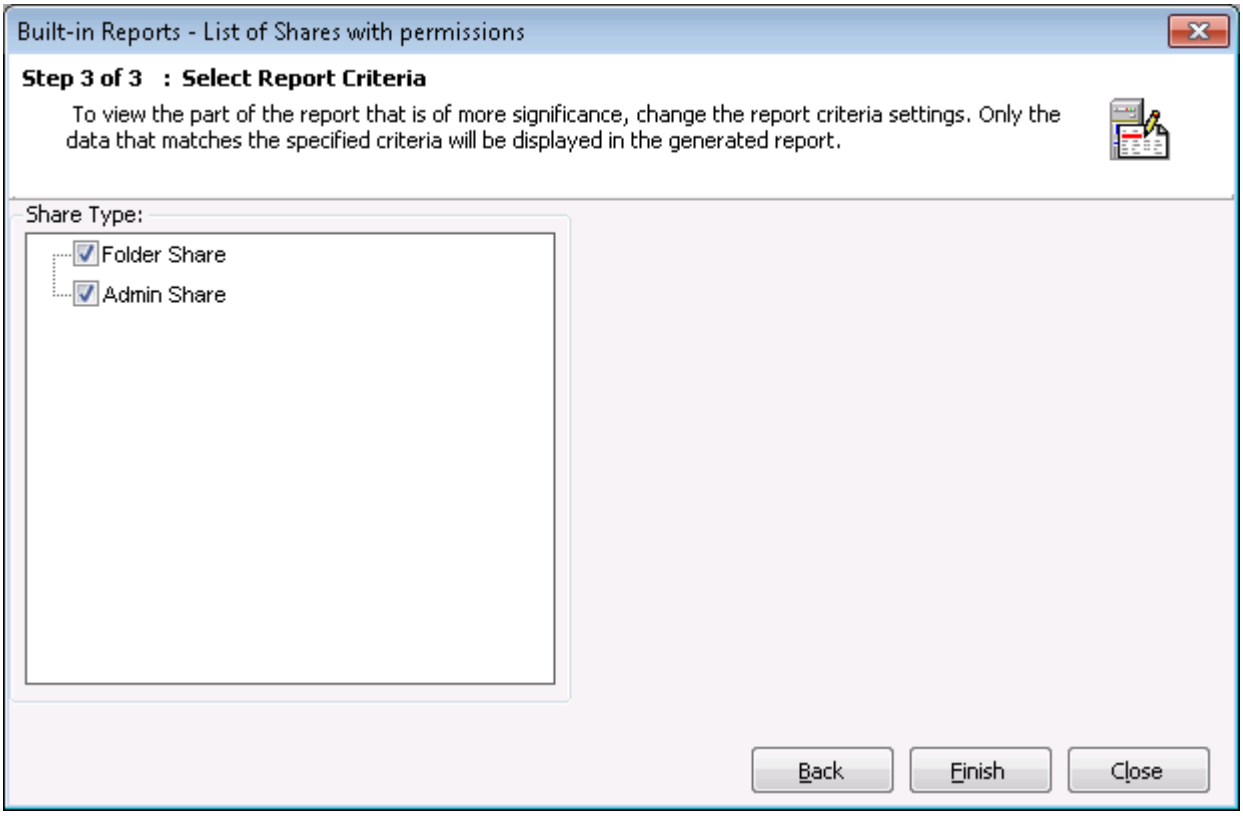
The default option selected is All Domains, for all the reports.


Built-in Reports - List of Shares with permissions
Step 2 of 3 : Select Domain(s)/Server(s)
You can either generate the report across domains by selecting All Domains or for a specific domain/server by selecting the Select Domain/Server option. This report can also be generated specifically for a single server by selecting the Server option.
All Domains
Select Domain/Server
Add Domains
RESEARCHLAB
Domain Controllers
RD30
Servers/Workstations
VOYAGER
VSSPRO
Select Scan Profile:
--Select a Profile--
Back
Next
Close

Click **Next** to proceed to the next step.

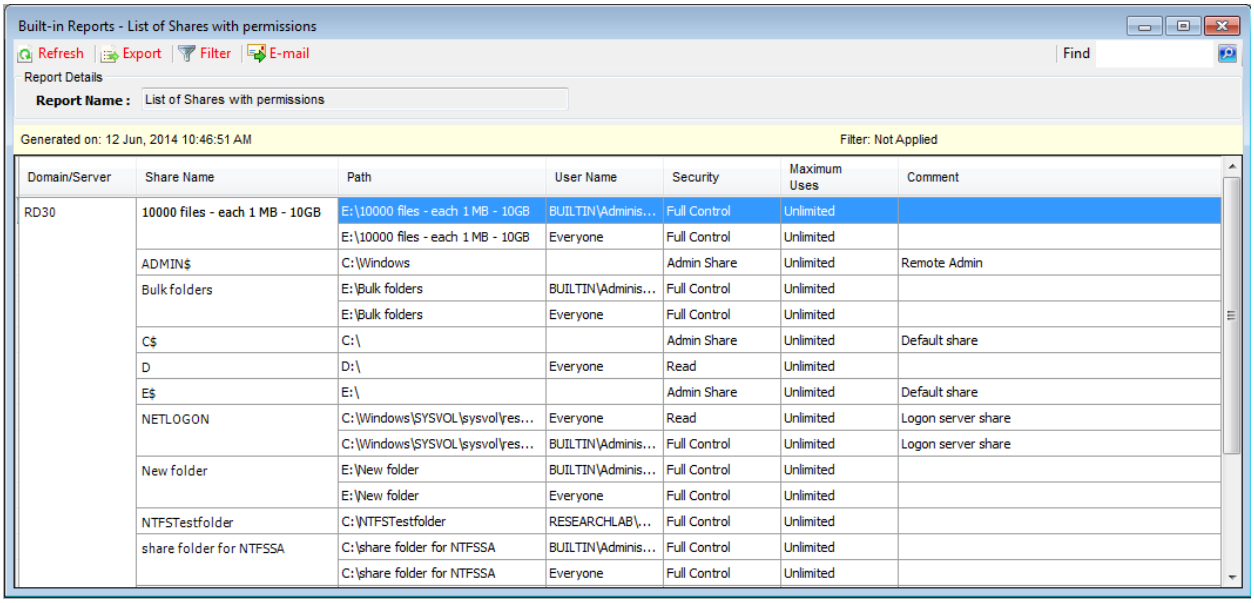
Step 3: Select Report Criteria

To view the part of the report that is of more significance, change the report criteria settings. Only the data that matches the specified criteria will be displayed in the generated report.


Built-in Reports - List of Shares with permissions
Step 3 of 3 : Select Report Criteria
To view the part of the report that is of more significance, change the report criteria settings. Only the data that matches the specified criteria will be displayed in the generated report.
Share Type:
Folder Share
Admin Share
Back
Finish
Close

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



Domain/Server	Share Name	Path	User Name	Security	Maximum Uses	Comment
RD30	10000 files - each 1 MB - 10GB	E:\10000 files - each 1 MB - 10GB	BUILTIN\Adminis...	Full Control	Unlimited	
		E:\10000 files - each 1 MB - 10GB	Everyone	Full Control	Unlimited	
	ADMIN$	C:\Windows		Admin Share	Unlimited	Remote Admin
	Bulk folders	E:\Bulk folders	BUILTIN\Adminis...	Full Control	Unlimited	
		E:\Bulk folders	Everyone	Full Control	Unlimited	
	C$	C:\		Admin Share	Unlimited	Default share
	D	D:\	Everyone	Read	Unlimited	
	E$	E:\		Admin Share	Unlimited	Default share
	NETLOGON	C:\Windows\SYSVOL\sysvol\res...	Everyone	Read	Unlimited	Logon server share
		C:\Windows\SYSVOL\sysvol\res...	BUILTIN\Adminis...	Full Control	Unlimited	Logon server share
	New folder	E:\New folder	BUILTIN\Adminis...	Full Control	Unlimited	
		E:\New folder	Everyone	Full Control	Unlimited	
	NTFSTestfolder	C:\NTFSTestfolder	RESEARCHLAB\...	Full Control	Unlimited	
	share folder for NTFSSA	C:\share folder for NTFSSA	BUILTIN\Adminis...	Full Control	Unlimited	
		C:\share folder for NTFSSA	Everyone	Full Control	Unlimited	

List of Reports:

Report Name	Description
List of Shares	Reports all the shares and their properties excluding the permission information.
List of Shares with permissions	Reports all the shares and their properties including the permission information.

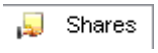
Shares, Folders and Files

How to view Shares, Folders and Files information?

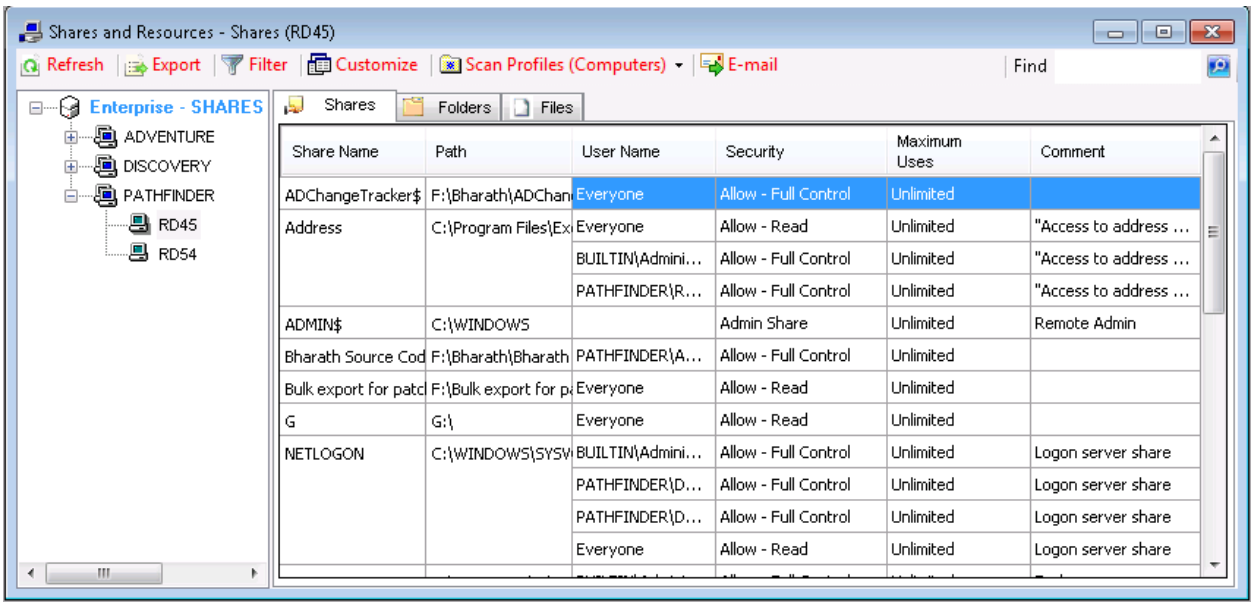
How to view Shares, Folders and Files information?

Click on

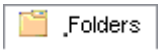
button to view information available under each tab as listed below.

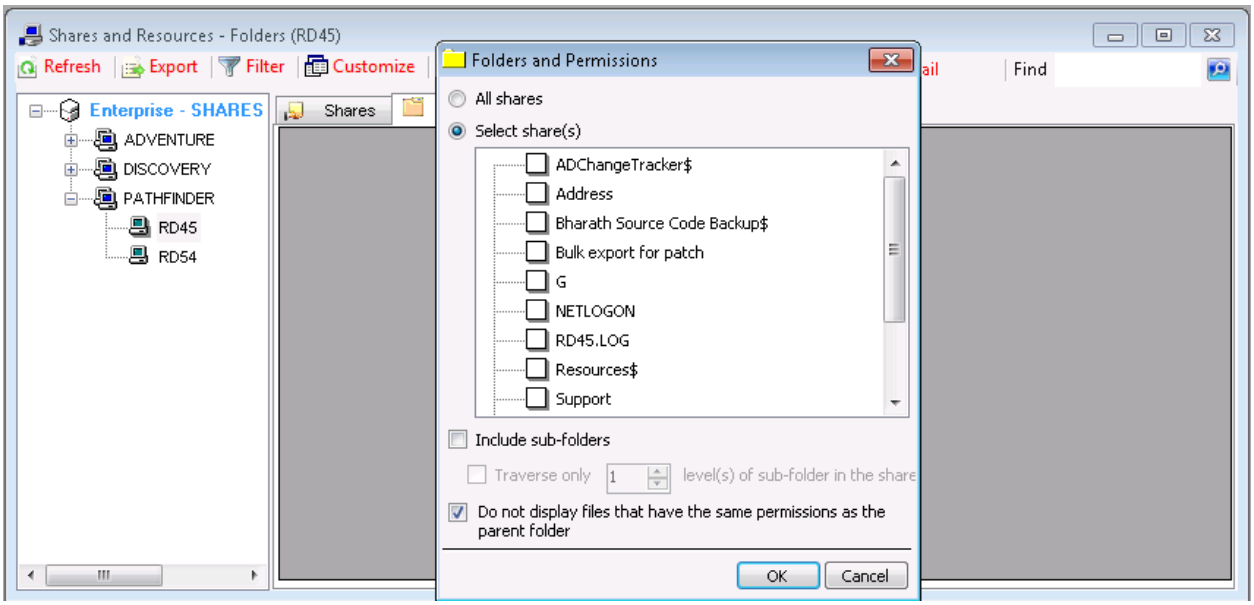
Click 

tab to view the following information: Share Name, Path, User Name, Security, Maximum, Comment.


Shares and Resources - Shares (RD45)
Refresh
Export
Filter
Customize
Scan Profiles (Computers)
E-mail
Find
Enterprise - SHARES
ADVENTURE
DISCOVERY
PATHFINDER
RD45
RD54
Shares
Folders
Files
Share Name
Path
User Name
Security
Maximum Uses
Comment
ADChangeTracker$ F:\Bharath\ADChan Everyone Allow - Full Control Unlimited
Address C:\Program Files\Ex Everyone Allow - Read Unlimited "Access to address ...
BUILTIN\Admini... Allow - Full Control Unlimited "Access to address ...
PATHFINDER\R... Allow - Full Control Unlimited "Access to address ...
ADMIN$ C:\WINDOWS Admin Share Unlimited Remote Admin
Bharath Source Cod F:\Bharath\Bharath PATHFINDER\A... Allow - Full Control Unlimited
Bulk export for patc F:\Bulk export for p Everyone Allow - Read Unlimited
G G:\ Everyone Allow - Read Unlimited
NETLOGON C:\WINDOWS\SYSV BUILTIN\Admini... Allow - Full Control Unlimited Logon server share
PATHFINDER\D... Allow - Full Control Unlimited Logon server share
PATHFINDER\D... Allow - Full Control Unlimited Logon server share
Everyone Allow - Read Unlimited Logon server share

How to view permissions of folders in a share?

Click  tab. The Folders and Permissions dialog appears.



You can view permissions of folder(s) in a share or for all the shares in the selected server by selecting “All shares” option or “Select share(s)” option respectively.

You can also optionally include the sub-folder(s) information by selecting the “Include sub-folders” option.

The sub-folder(s) having permissions identical as the parent folder would be shown in bold text with "Same as parent" in both User Name and Security fields in the report. If you do not want folders with identical permissions as the parent folder reported, then select, the "Do not display folders that have same permissions as the parent folder" option. This option will not report folders with identical permissions as the parent folder.

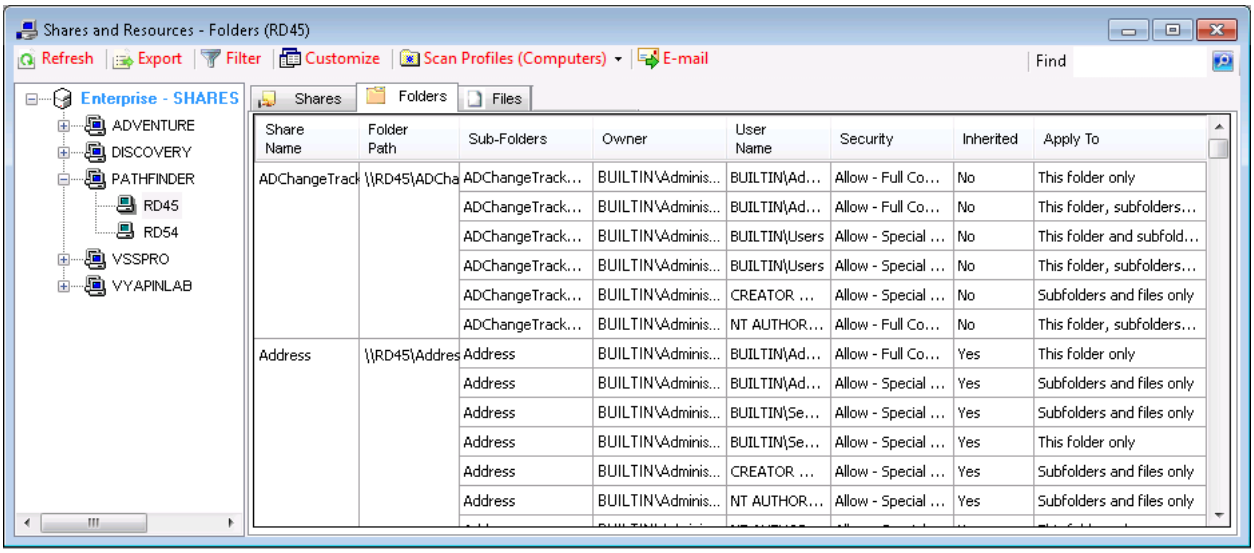
To view up to a certain level of sub-folders, select the "Traverse only 'n' level(s) of sub-folder in the share" option and specify a sub-folder level, Where the levels are numbered as follows:

\\server\sharename\Level 1\Level 2\Level 3...

Note: The "Include sub-folders" option defaults to enumerating all the sub-folders unless you specify a sub-folder level in "Traverse only 'n' level(s) of sub-folder in the share" option.

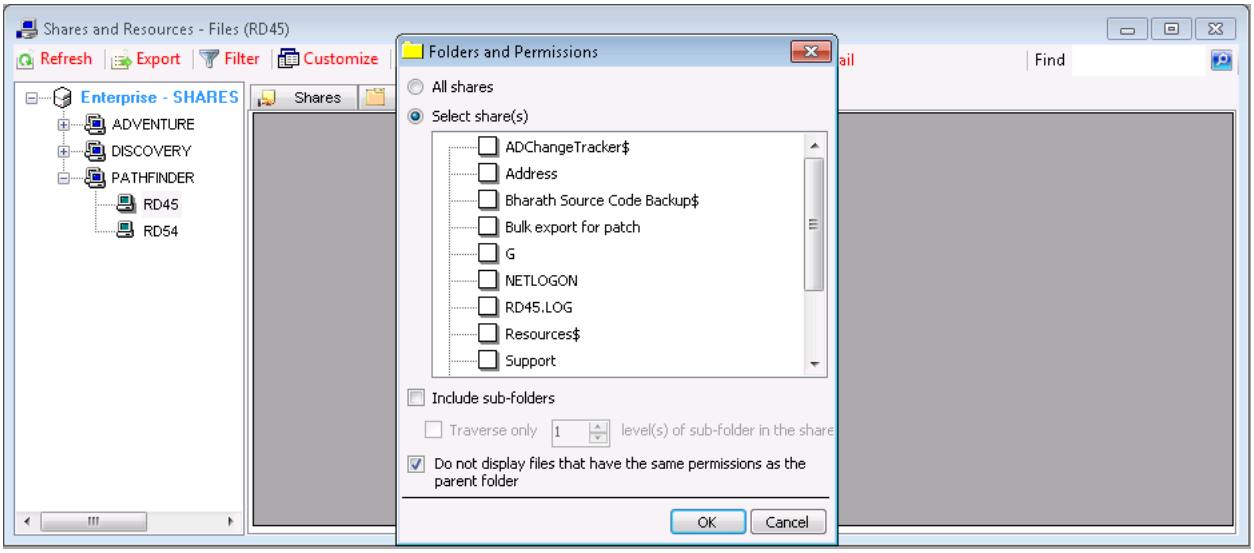
Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

The report would be displayed as below:



How to view permissions of files in a share?

Click tab. The "Files and Permissions" dialog appears.



You can view permissions of files in a share or for all the shares in the selected server by selecting "All shares" option or "Select share(s)" option respectively.

You can also optionally include the sub-folder(s) information by selecting the "Include sub-folders" option.

The files having permissions identical to the parent folder would show up with "Same as parent" in both User Name and Security fields in the report. If you do not want files with identical permissions as the parent folder reported, then select, the "Do not display files that have same permissions as the parent folder" option. This option will not report files with identical permissions as the parent folder.

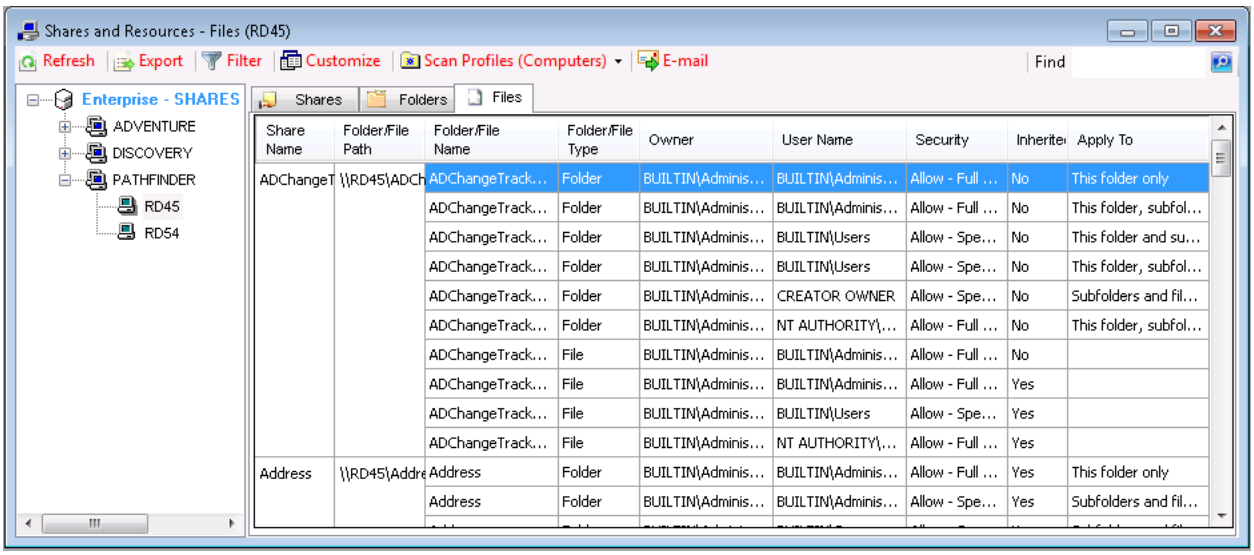
To view up to a certain level of sub-folders and files, select the "Traverse only 'n' level(s) of sub-folder in the share" option and specify a sub-folder level, where the levels are numbered as follows:

\\server\sharename\Level 1\Level 2\Level 3...

Note: The "Include sub-folders" option defaults to enumerating all the sub-folders unless you specify a sub-folder level in "Traverse only 'n' level(s) of sub-folder in the share" option.

Note: The "Do not display files that have same permissions as the parent folder" option would be enabled by default.

The report would be displayed as below:



DAC Reports

About DAC Reports

How to view the effective DAC permissions for specified accounts?

How to view the effective DAC permissions for the selected set of shared folder?

How to view the Central Access Policies and policies permissions?

How to check the shared folder and subfolders affected by DAC policies?

About DAC Reports

The DAC Reports feature provides many options to view the Dynamic Access Control (DAC) effective permissions on shared Folders. You may view the selected Account effective DAC permissions on shared folders and the associated effective DAC permissions for specific folders. You may also check the folders affected/not affected by DAC Central Access Policies and view the Central Access Policy and Central Access Rule (CAR) available on the selected Domain/Server. Here are some examples of how you may make effective use of this feature:

1. Determine what type of permissions and conditions have been configured for each the Central Access Rules in Central Access policy over the domain.
2. Search on who have access limited permissions by DAC on which folders.
3. Select a set of accounts and determine for which shared folders they have DAC permissions.
4. Determine on which shared folders and subfolders have been affected/not affected by the Central Access Policy.
5. Select a Set of Domain(s)/Server(s) and determine the configured Central Access Policies and Central Access Rules.

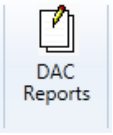
The DAC reports feature provides reports in the following categories:

Report Name	Description
Effective DAC permissions for specific users and groups on folders	Reports the effective DAC permissions for the specified users and groups.
Effective DAC permissions for Accounts having permissions on specific folders	Reports the effective DAC permissions for the specified folders.
List of Central Access Policies (CAP) and Central Access Rules on the Domain	Reports the Central Access Policies (CAP) and Central Access Rules configured for a domain.
Folders affected/not affected by DAC Central Access Policies	Reports the folders affected/not affected by the DAC Central Access Policy and Central Access Rules.

Note: The DAC Reports feature can run on Windows 8, Windows 8.1, Windows Sever 2012 and Windows Server 2012 R2 computers only.

How to view the effective DAC permissions for the specified accounts?

Effective DAC permissions for specific users and groups on folders:

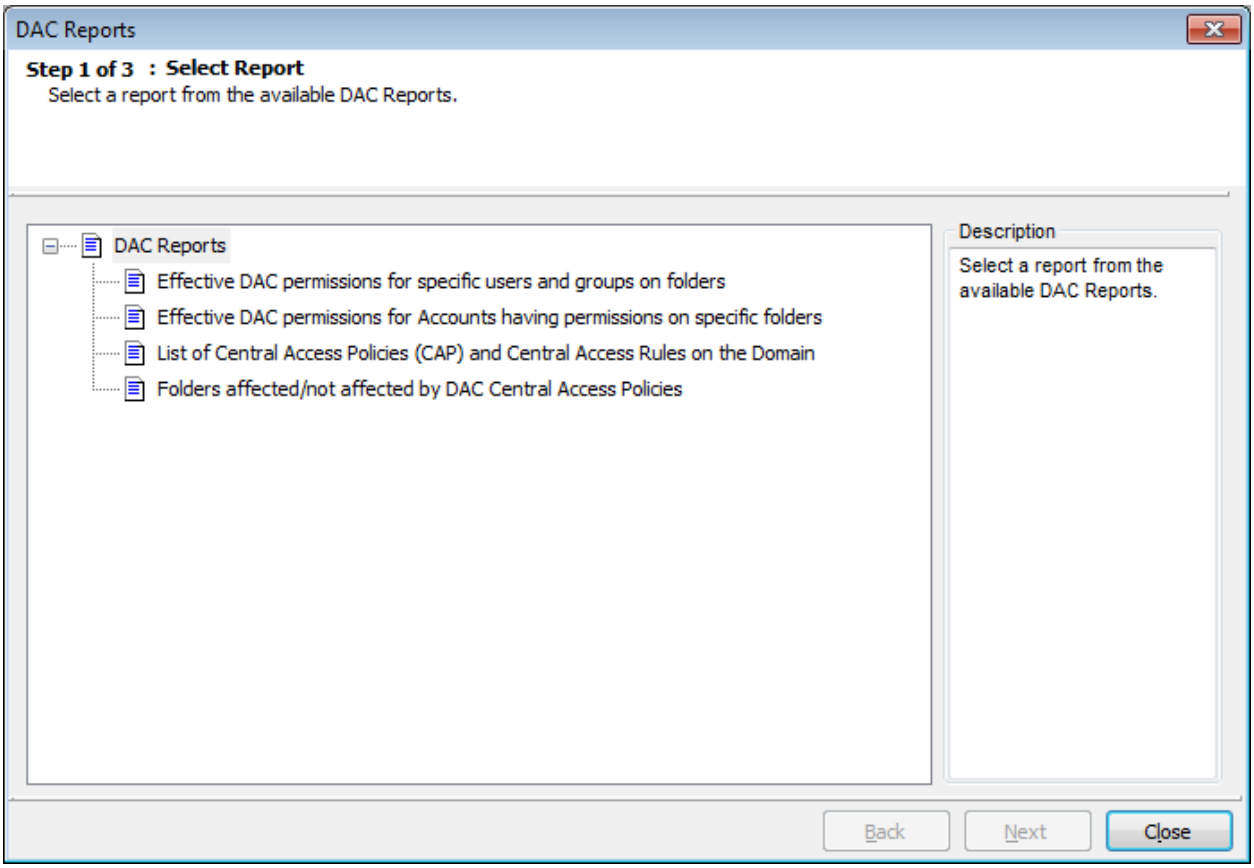
Click on 

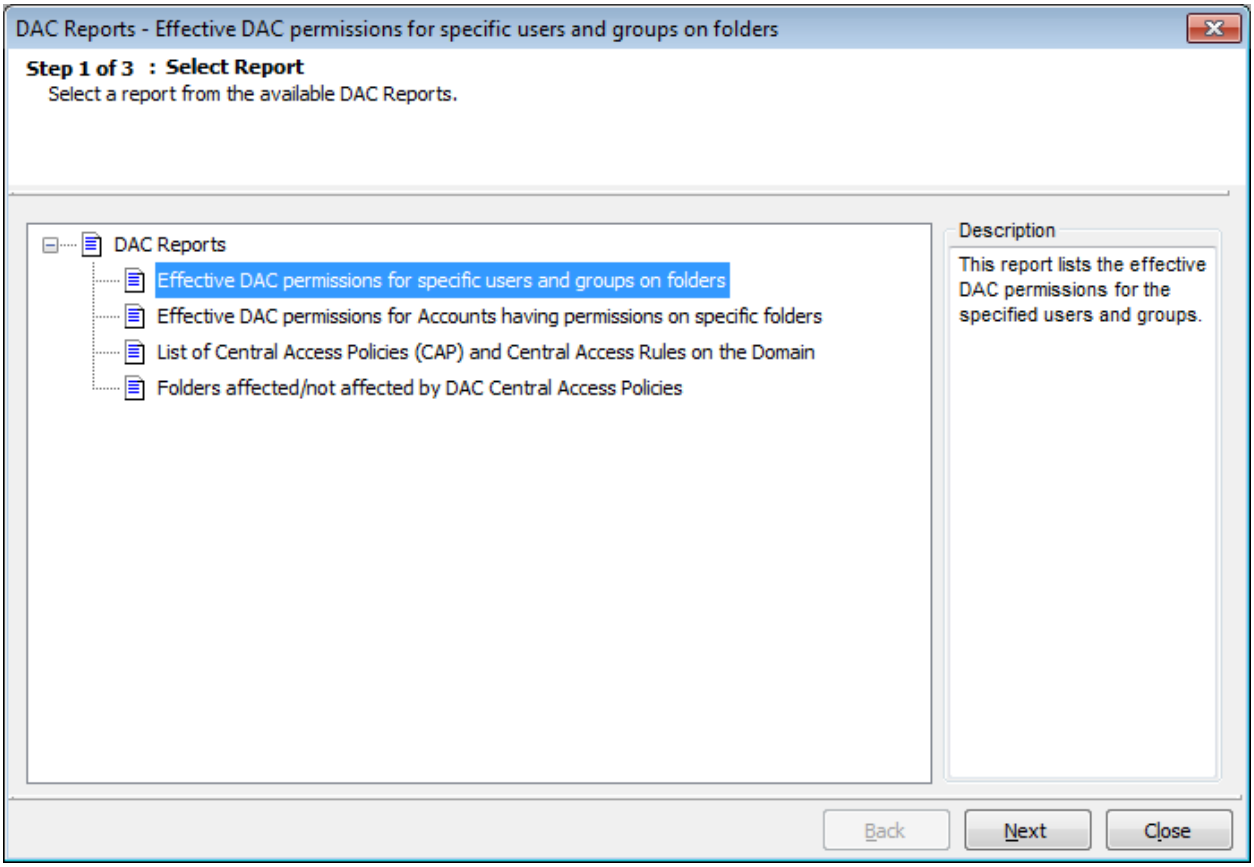
button.

The DAC Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

Select the report to be generated. Only one report can be generated at a time.

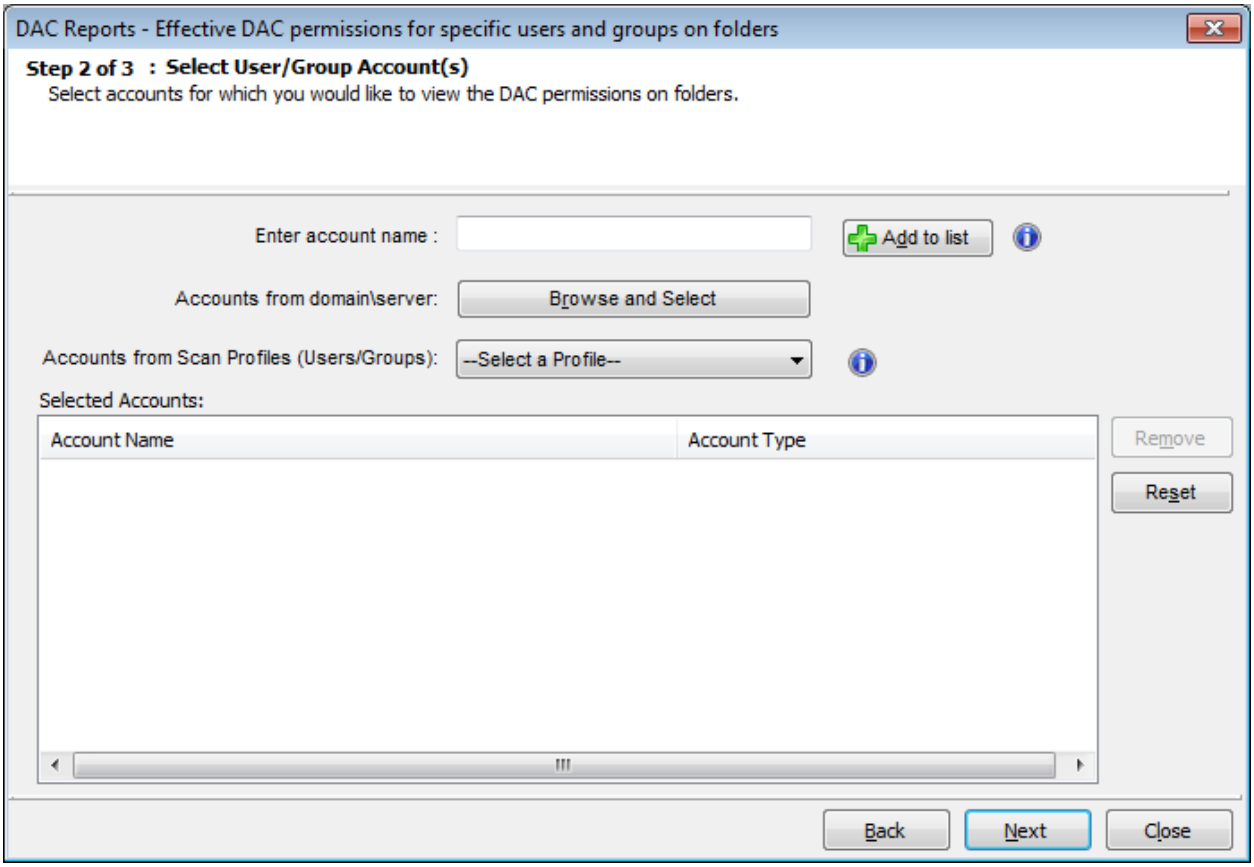

DAC Reports
Step 1 of 3 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
Select a report from the available DAC Reports.
Back
Next
Close


DAC Reports - Effective DAC permissions for specific users and groups on folders
Step 1 of 3 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
This report lists the effective DAC permissions for the specified users and groups.
Back
Next
Close

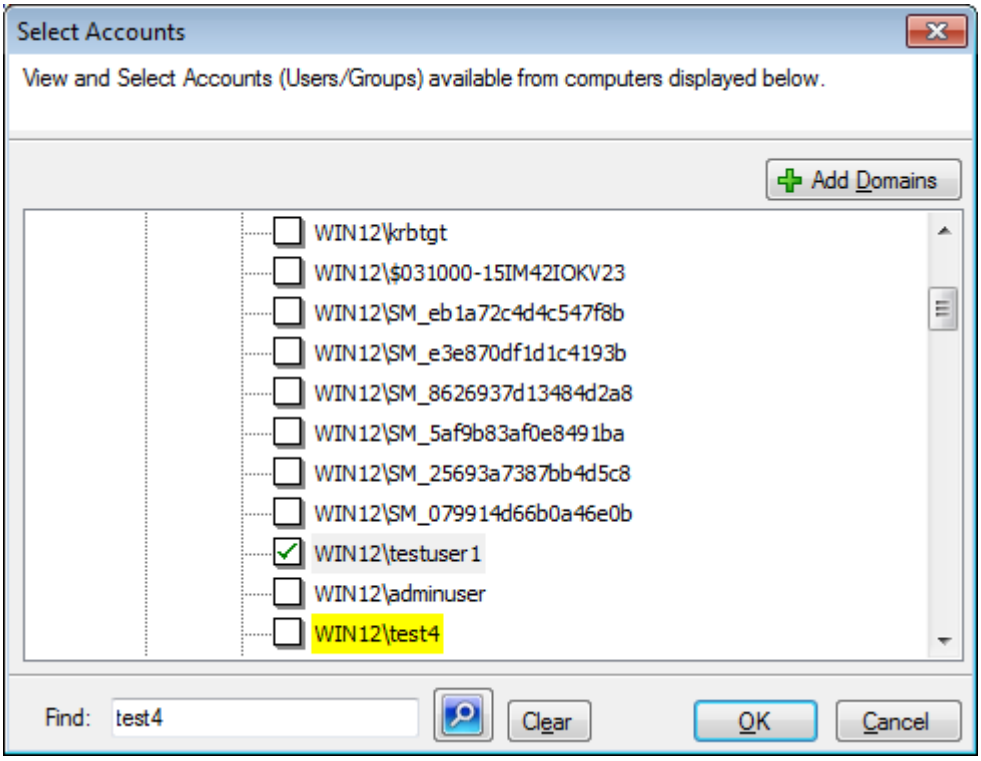
Click **Next** to proceed to the next step.

Step 2: Account Selection

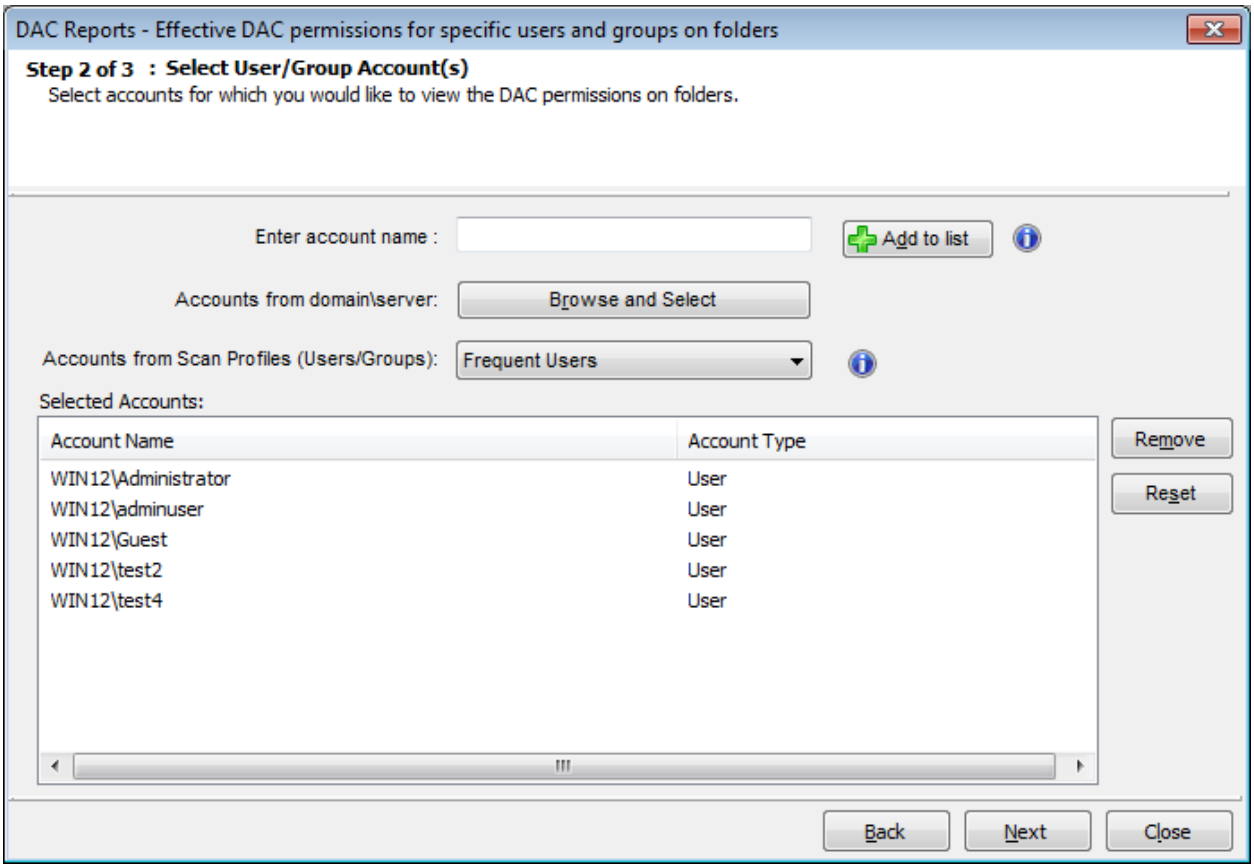
1. Select the accounts, for which you wish to view the DAC permissions.
2. The selected accounts will be added to the wizard as shown below:



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list.
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click **About Scan Profiles (Users/Groups)**.
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).



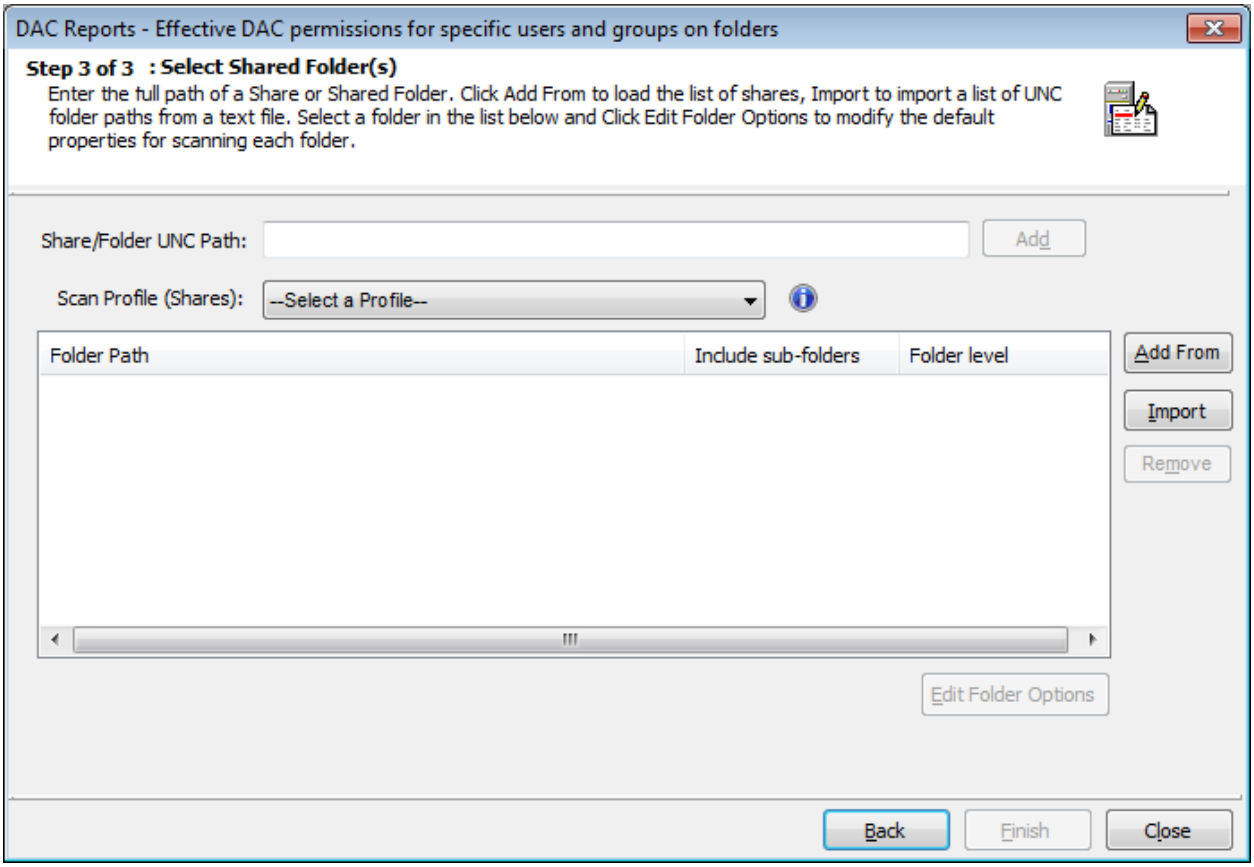
- Use the **Find** option to search desired user/group accounts.



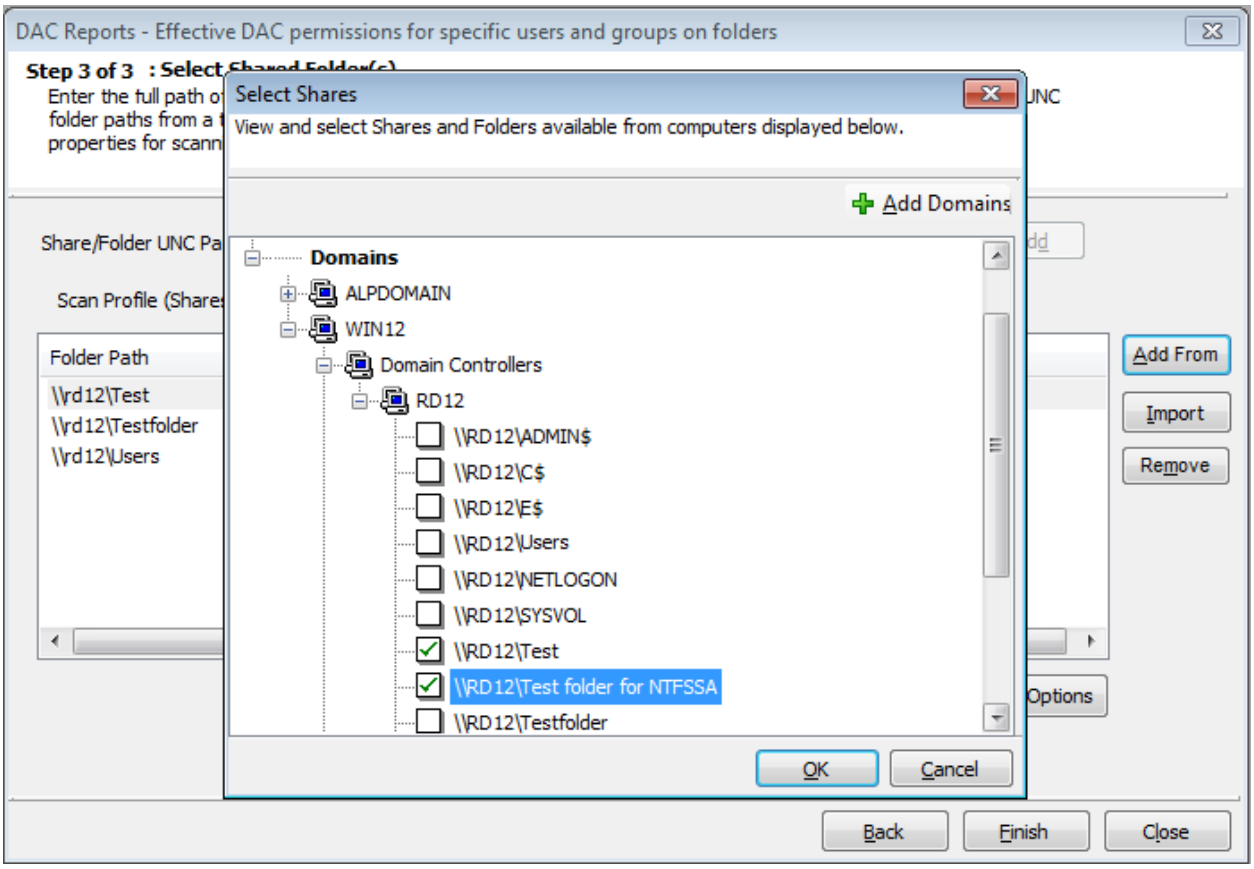
Click **Next** to proceed.

Step 3: Select Shared Folders

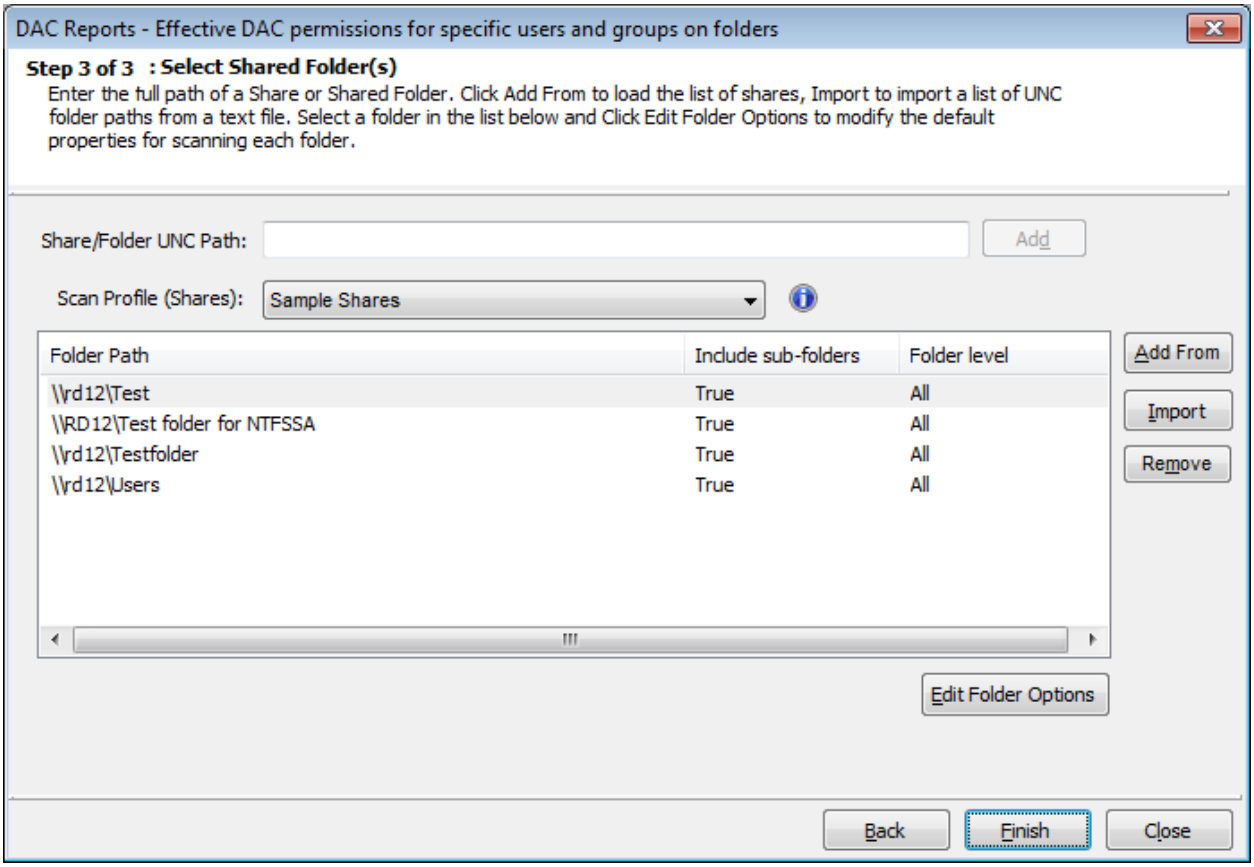
Select shared folder(s) by using any of the input options displayed.


DAC Reports - Effective DAC permissions for specific users and groups on folders
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Edit Folder Options
Back
Finish
Close

- Click the option **Add From**
- Select one or more servers to enumerate its shared folders.

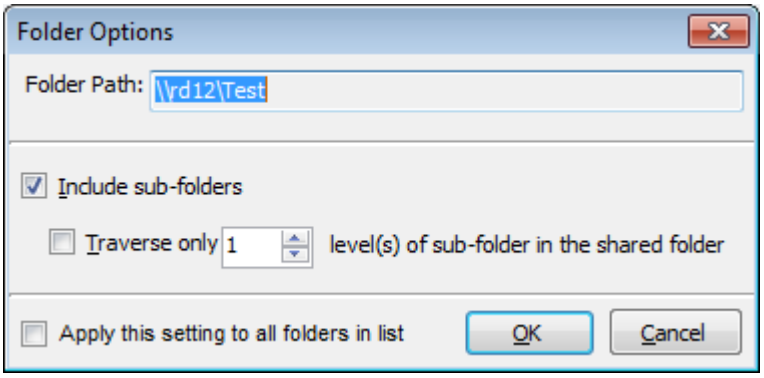


- Use **Select a Profile** option to use the shares added in the profile.



You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

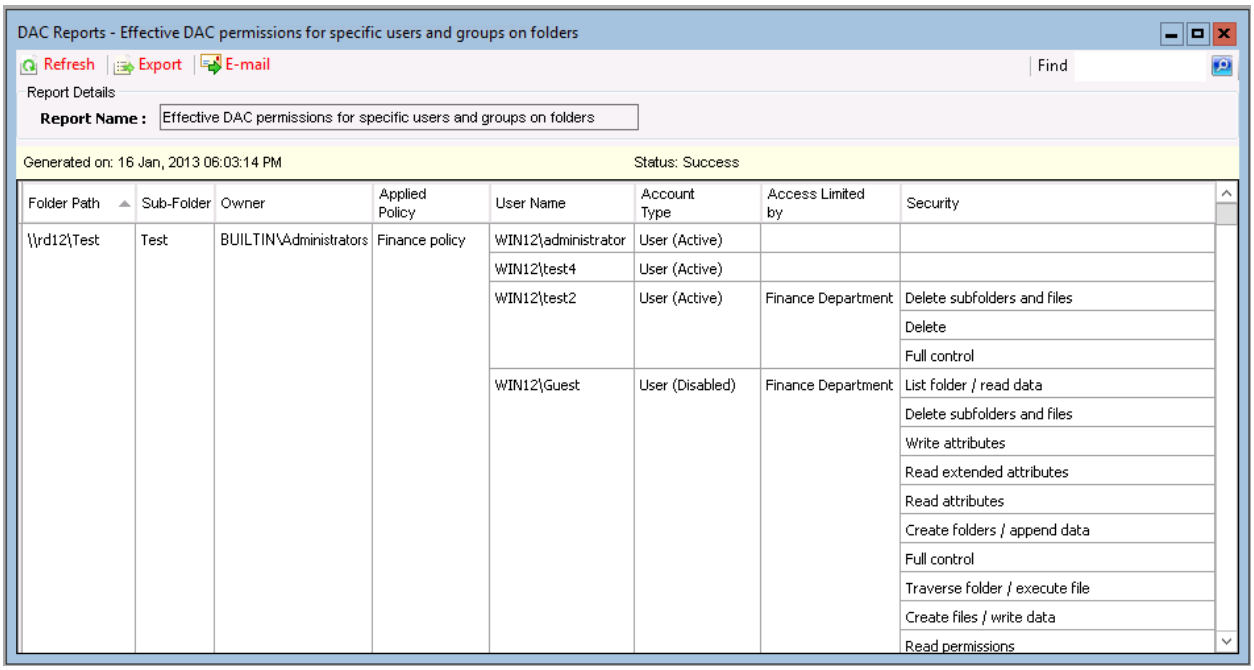
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

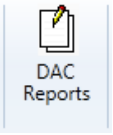
After the data collection process is complete, the report would be generated in a report window as shown below:


DAC Reports - Effective DAC permissions for specific users and groups on folders
Refresh
Export
E-mail
Find
Report Details
Report Name :
Effective DAC permissions for specific users and groups on folders
Generated on: 16 Jan, 2013 06:03:14 PM
Status: Success

Folder Path	Sub-Folder	Owner	Applied Policy	User Name	Account Type	Access Limited by	Security
\\rd12\Test	Test	BUILTIN\Administrators	Finance policy	WIN12\administrator	User (Active)		
				WIN12\test4	User (Active)		
				WIN12\test2	User (Active)	Finance Department	Delete subfolders and files
							Delete
							Full control
				WIN12\Guest	User (Disabled)	Finance Department	List folder / read data
							Delete subfolders and files
							Write attributes
							Read extended attributes
							Read attributes
							Create folders / append data
							Full control
							Traverse folder / execute file
							Create files / write data
							Read permissions

How to view the effective DAC permissions for Accounts having permissions on specific folders?

Effective DAC permissions for Accounts having permissions on specific folders:

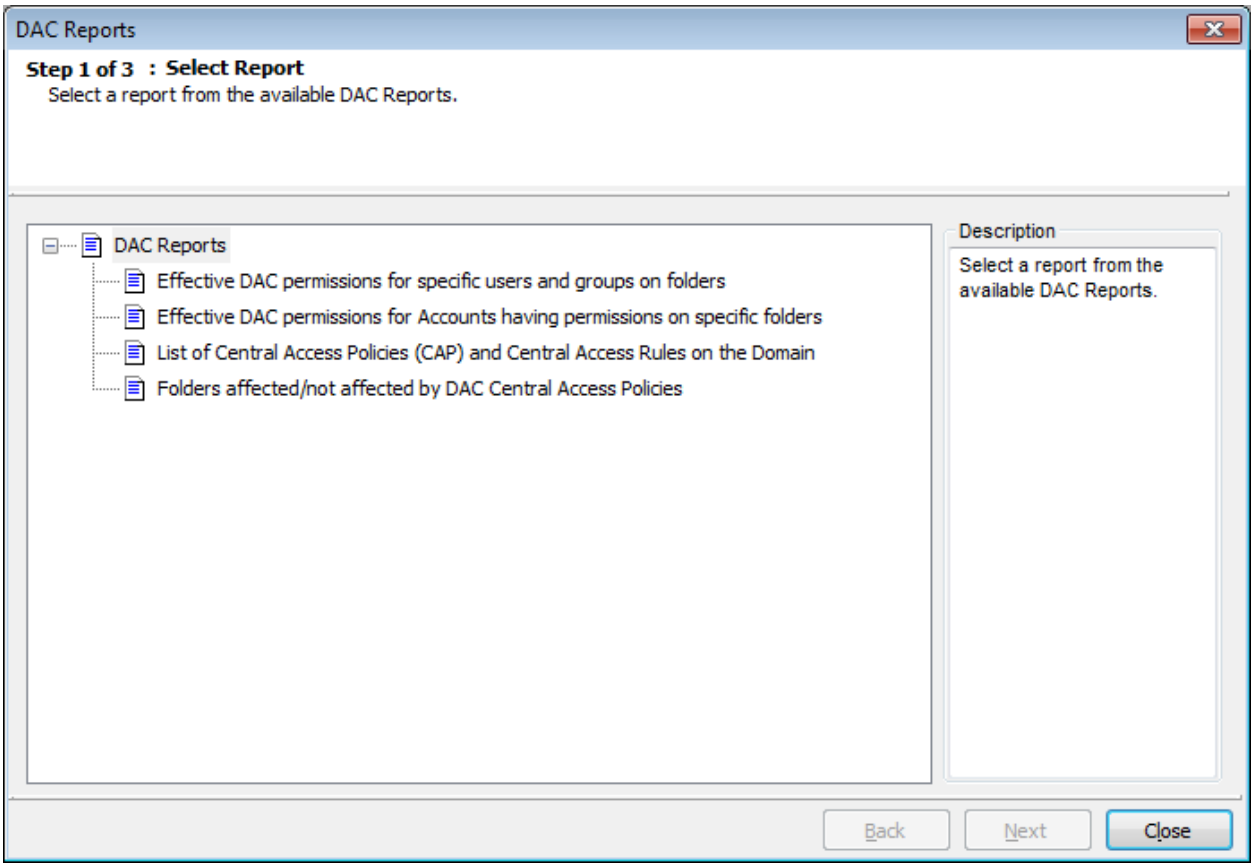
Click on 

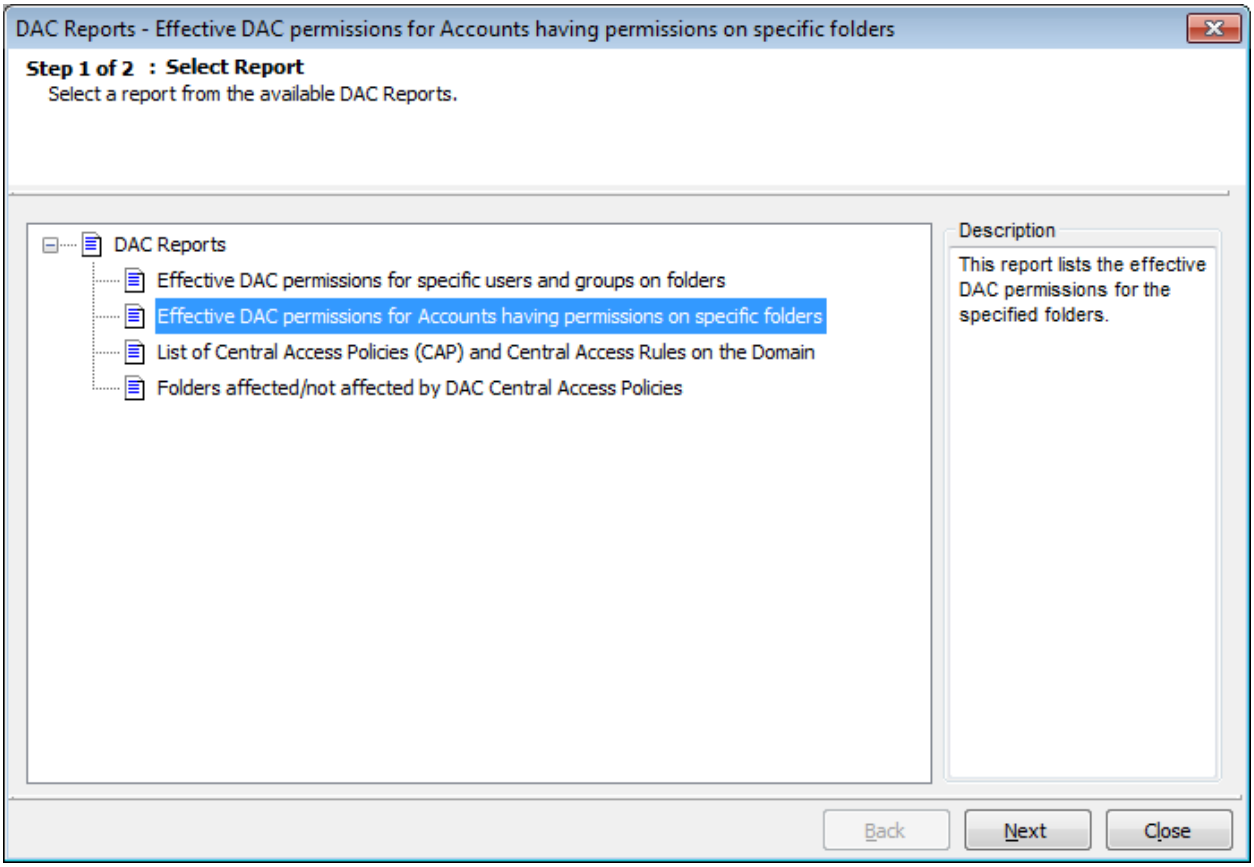
button.

The DAC Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

Select the report to be generated. Only one report can be generated at a time.

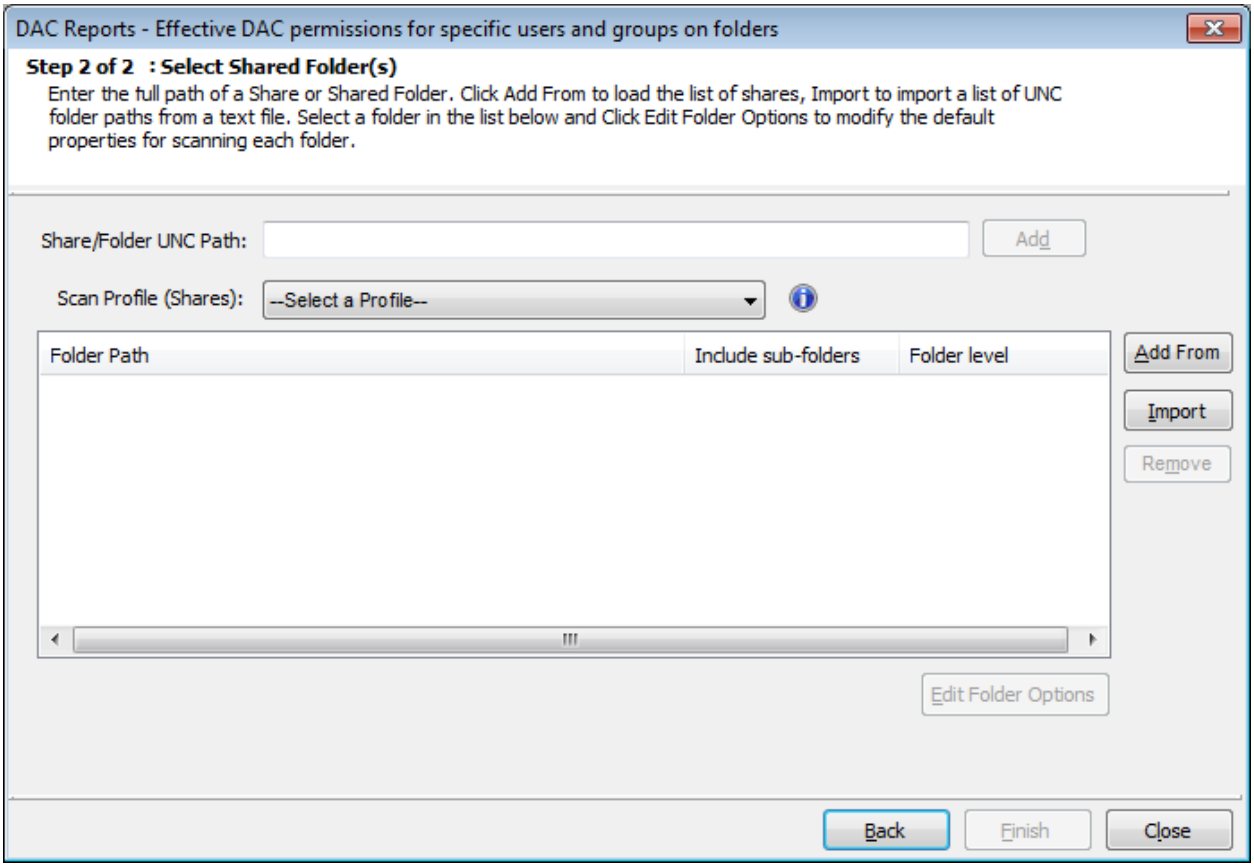

DAC Reports
Step 1 of 3 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
Select a report from the available DAC Reports.
Back
Next
Close


DAC Reports - Effective DAC permissions for Accounts having permissions on specific folders
Step 1 of 2 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
This report lists the effective DAC permissions for the specified folders.
Back
Next
Close

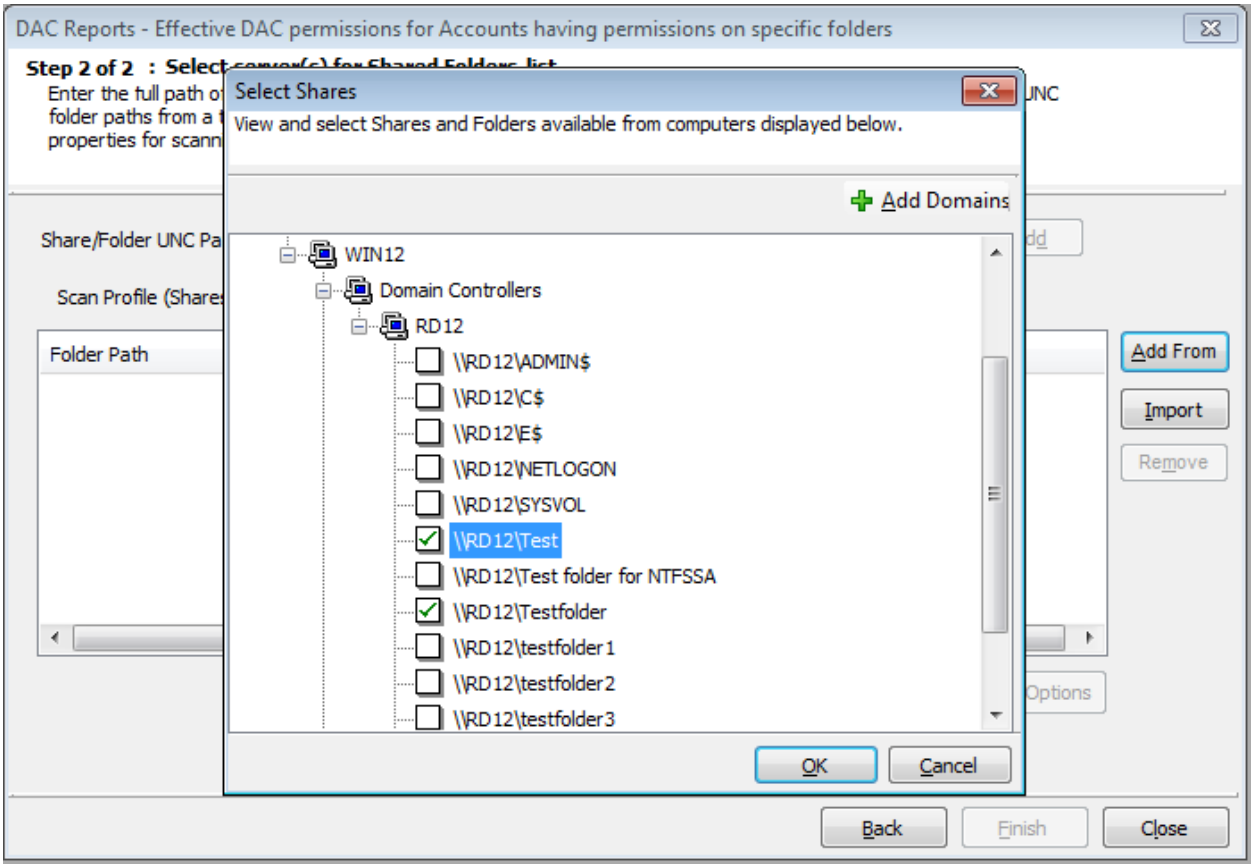
Click **Next** to proceed to the next step.

Step 2: Select shared folders

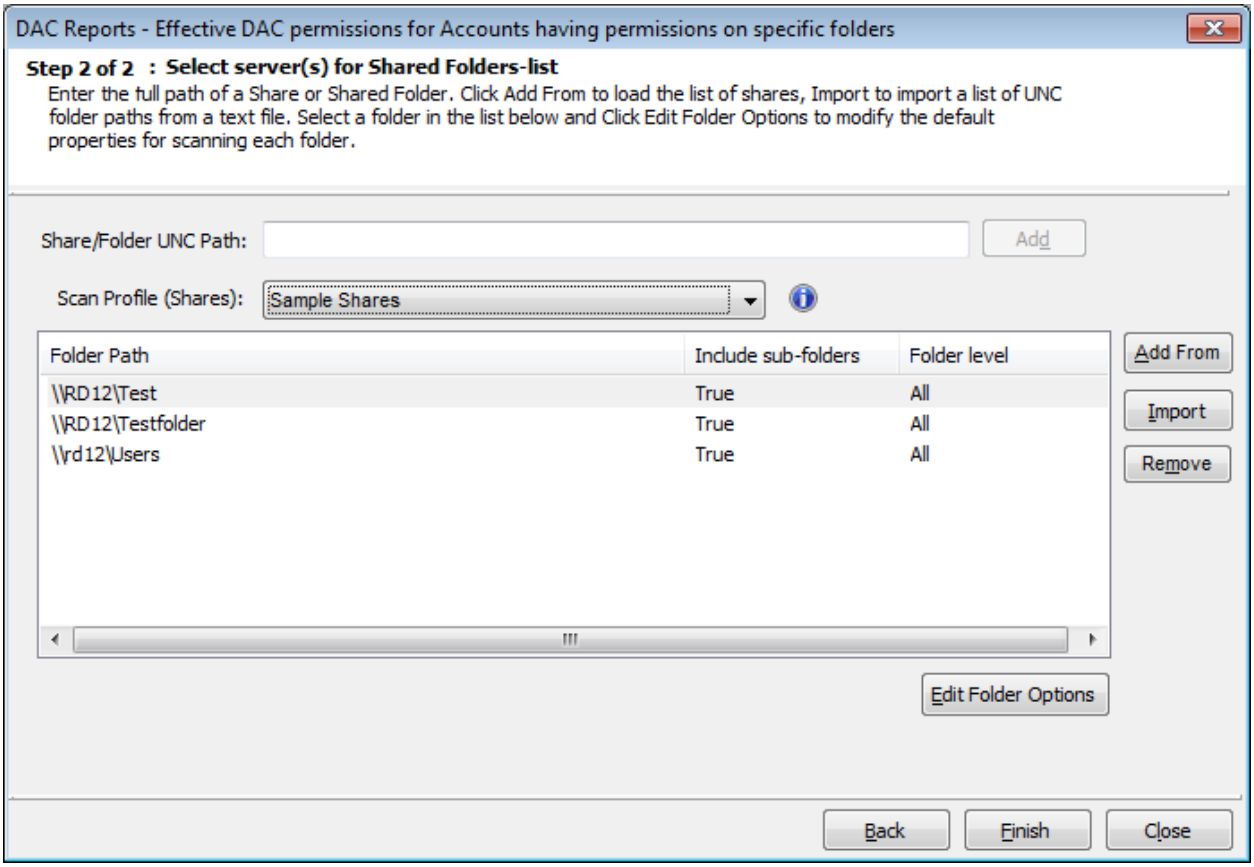
Select shared folder(s) by using any of the input options displayed.


DAC Reports - Effective DAC permissions for specific users and groups on folders
Step 2 of 2 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Edit Folder Options
Back
Finish
Close

- Click the option **Add From**
- Select one or more servers to enumerate its shared folders.

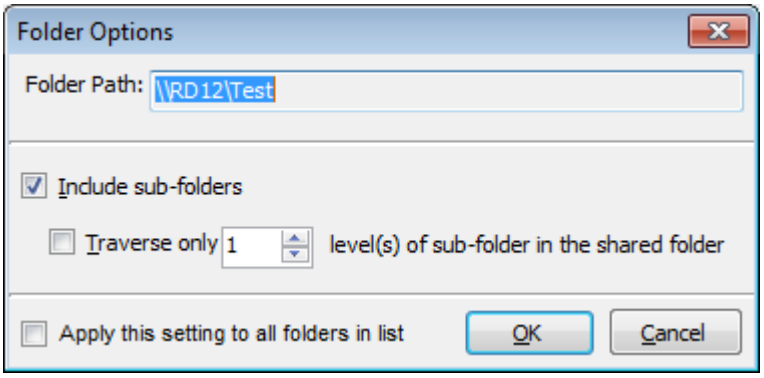


- Use **Select a Profile** option to use the shares added in the profile.


DAC Reports - Effective DAC permissions for Accounts having permissions on specific folders
Step 2 of 2 : Select server(s) for Shared Folders-list
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
Sample Shares
Folder Path
Include sub-folders
Folder level
\\RD12\Test
True
All
\\RD12\Testfolder
True
All
\\rd12\Users
True
All
Add From
Import
Remove
Edit Folder Options
Back
Finish
Close

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

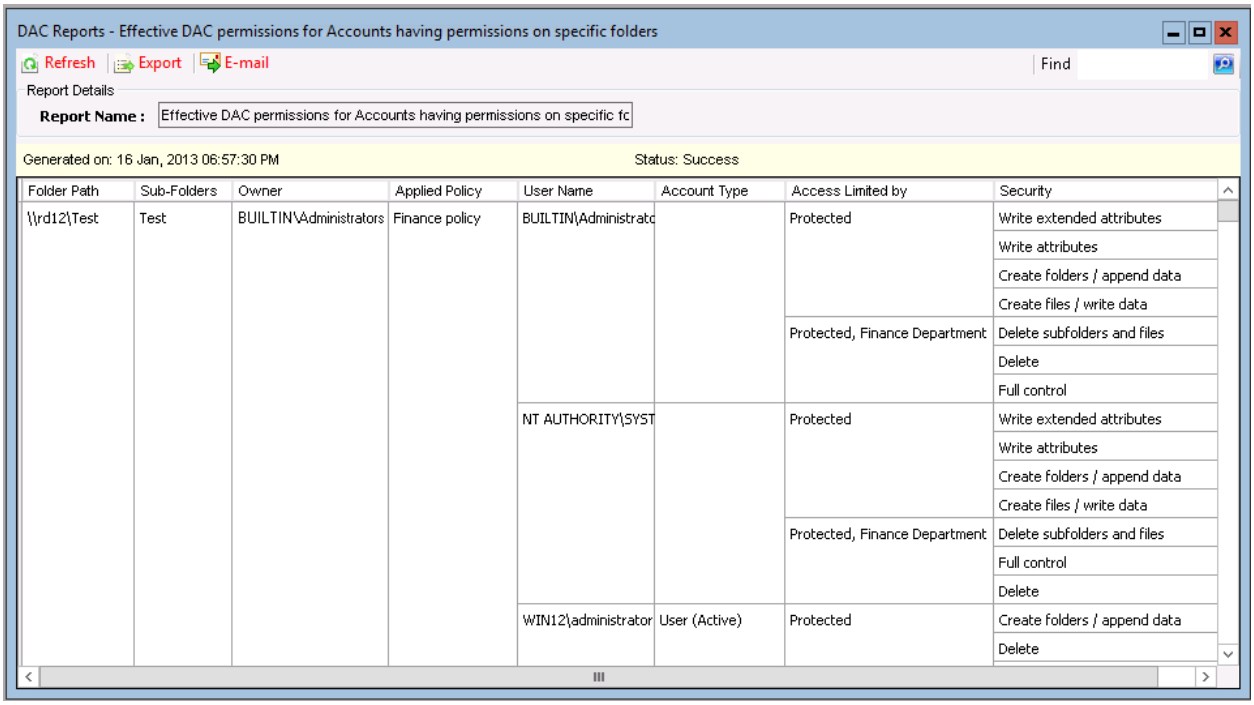
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

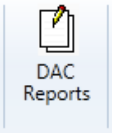
After the data collection process is complete, the report would be generated in a report window as shown below:


DAC Reports - Effective DAC permissions for Accounts having permissions on specific folders
Refresh
Export
E-mail
Find
Report Details
Report Name :
Effective DAC permissions for Accounts having permissions on specific fc
Generated on: 16 Jan, 2013 06:57:30 PM
Status: Success

Folder Path	Sub-Folders	Owner	Applied Policy	User Name	Account Type	Access Limited by	Security
\\rd12\Test	Test	BUILTIN\Administrators	Finance policy	BUILTIN\Administrato		Protected	Write extended attributes
							Write attributes
							Create folders / append data
							Create files / write data
						Protected, Finance Department	Delete subfolders and files
							Delete
							Full control
				NT AUTHORITY\SYST		Protected	Write extended attributes
							Write attributes
							Create folders / append data
							Create files / write data
						Protected, Finance Department	Delete subfolders and files
							Full control
							Delete
				WIN12\administrator	User (Active)	Protected	Create folders / append data
							Delete

How to view Central Access Policies and policy permissions?

List of Central Access Policies (CAP) and Central Access Rules on the Domain:

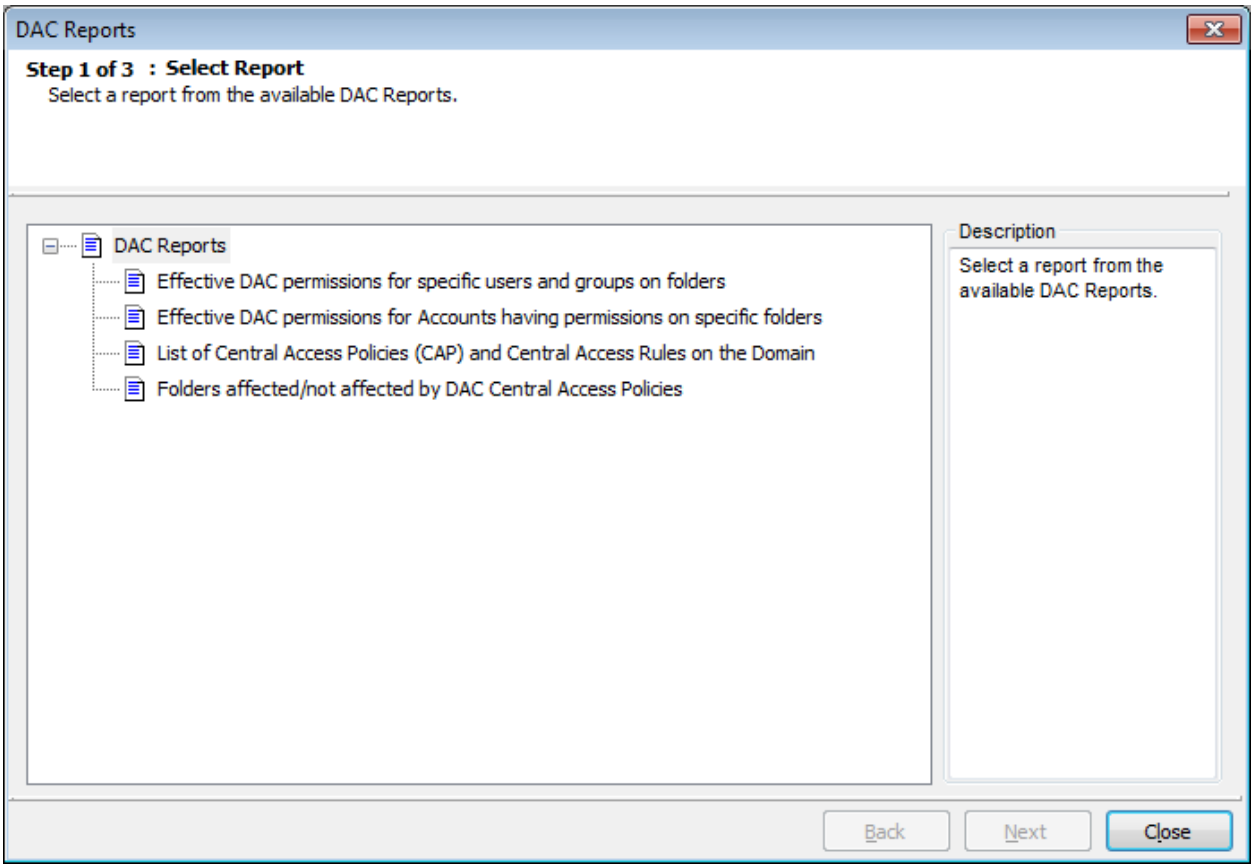
Click on 

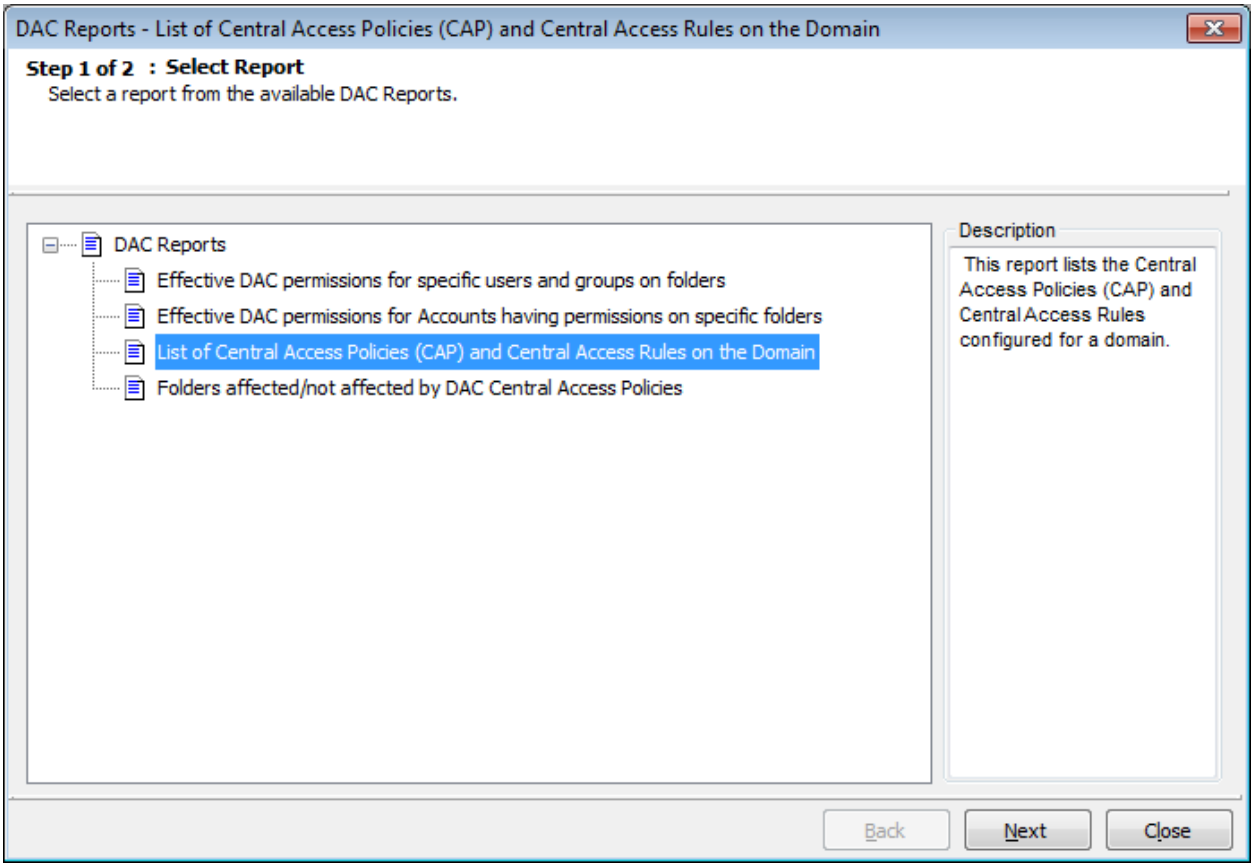
button.

The DAC Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

Select the report to be generated. Only one report can be generated at a time.

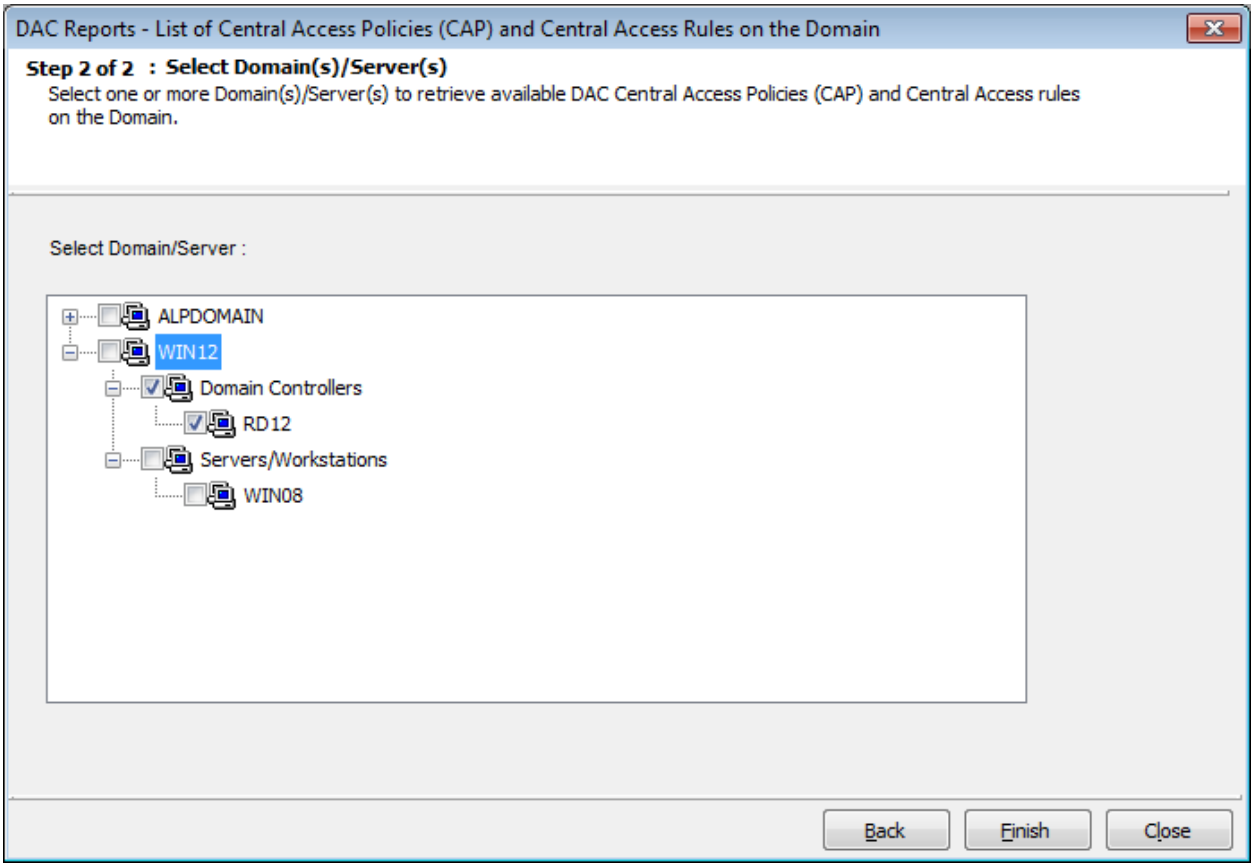

DAC Reports
Step 1 of 3 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
Select a report from the available DAC Reports.
Back
Next
Close


DAC Reports - List of Central Access Policies (CAP) and Central Access Rules on the Domain
Step 1 of 2 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
This report lists the Central Access Policies (CAP) and Central Access Rules configured for a domain.
Back
Next
Close

Click **Next** to proceed to the next step.

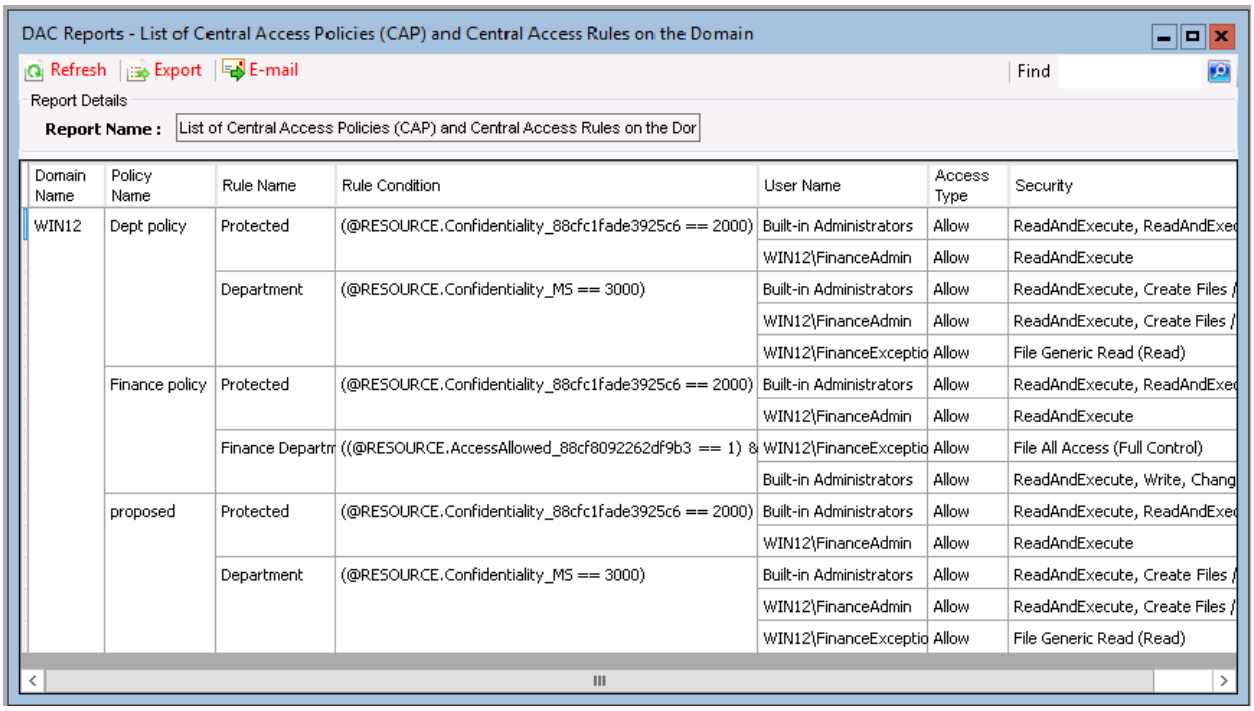
Step 2: Select Domain(s) / Server(s)

Select the Domain(s)/Server(s), for which the report needs to be generated.


DAC Reports - List of Central Access Policies (CAP) and Central Access Rules on the Domain
Step 2 of 2 : Select Domain(s)/Server(s)
Select one or more Domain(s)/Server(s) to retrieve available DAC Central Access Policies (CAP) and Central Access rules on the Domain.
Select Domain/Server :
ALPDOMAIN
WIN12
Domain Controllers
RD12
Servers/Workstations
WIN08
Back
Finish
Close

Click **Finish** to proceed to the next step.

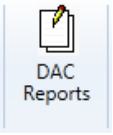
After the data collection process is complete, the report would be generated in a report window as shown below:


DAC Reports - List of Central Access Policies (CAP) and Central Access Rules on the Domain
Refresh
Export
E-mail
Find
Report Details
Report Name :
List of Central Access Policies (CAP) and Central Access Rules on the Dor

Domain Name	Policy Name	Rule Name	Rule Condition	User Name	Access Type	Security
WIN12	Dept policy	Protected	(@RESOURCE.Confidentiality_88cfc1fade3925c6 == 2000)	Built-in Administrators	Allow	ReadAndExecute, ReadAndExec
				WIN12\FinanceAdmin	Allow	ReadAndExecute
		Department	(@RESOURCE.Confidentiality_M5 == 3000)	Built-in Administrators	Allow	ReadAndExecute, Create Files /
				WIN12\FinanceAdmin	Allow	ReadAndExecute, Create Files /
				WIN12\FinanceExceptio	Allow	File Generic Read (Read)
	Finance policy	Protected	(@RESOURCE.Confidentiality_88cfc1fade3925c6 == 2000)	Built-in Administrators	Allow	ReadAndExecute, ReadAndExec
				WIN12\FinanceAdmin	Allow	ReadAndExecute
		Finance Departm	((@RESOURCE.AccessAllowed_88cf8092262df9b3 == 1) &	WIN12\FinanceExceptio	Allow	File All Access (Full Control)
				Built-in Administrators	Allow	ReadAndExecute, Write, Chang
	proposed	Protected	(@RESOURCE.Confidentiality_88cfc1fade3925c6 == 2000)	Built-in Administrators	Allow	ReadAndExecute, ReadAndExec
				WIN12\FinanceAdmin	Allow	ReadAndExecute
		Department	(@RESOURCE.Confidentiality_M5 == 3000)	Built-in Administrators	Allow	ReadAndExecute, Create Files /
				WIN12\FinanceAdmin	Allow	ReadAndExecute, Create Files /
				WIN12\FinanceExceptio	Allow	File Generic Read (Read)

How to check the shared folders and subfolders affected by DAC policies?

Folders affected/not affected by DAC Central Access Policies:

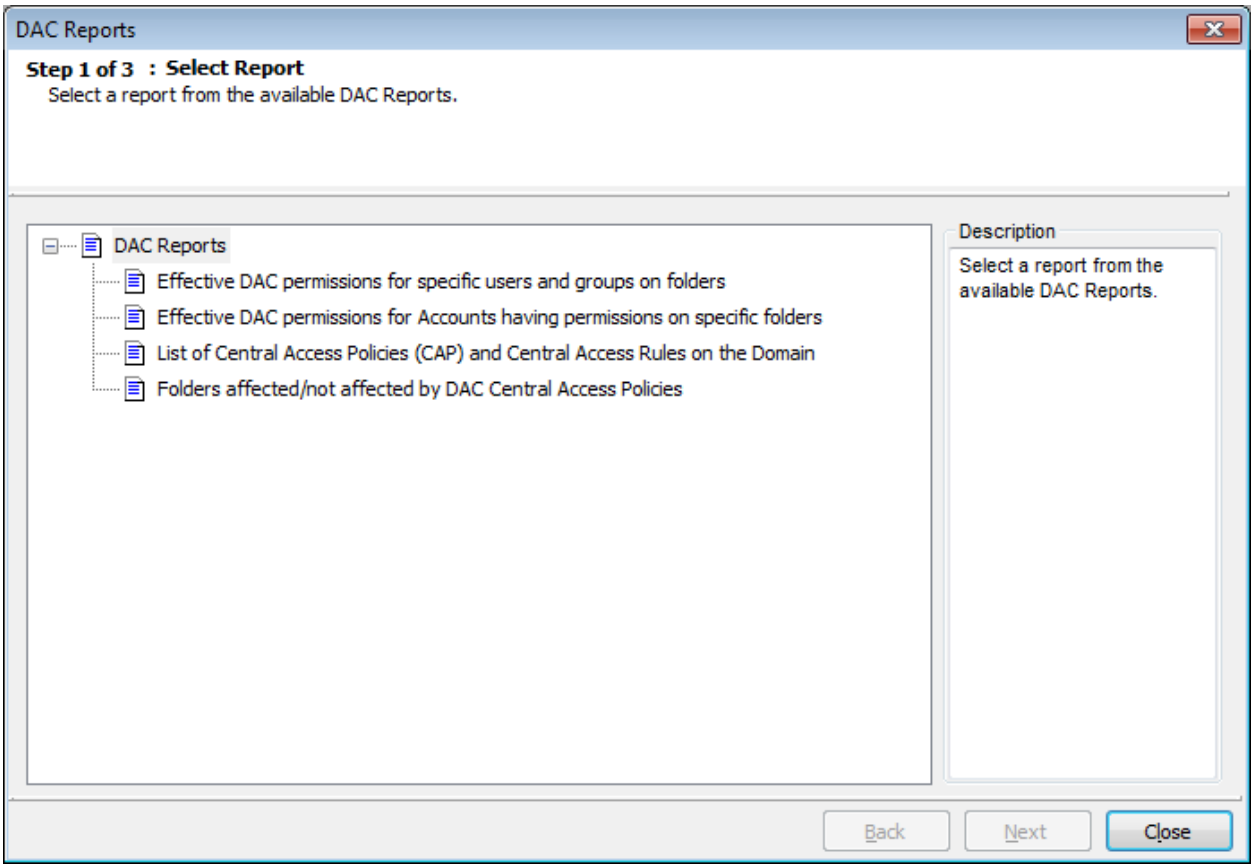
Click on 

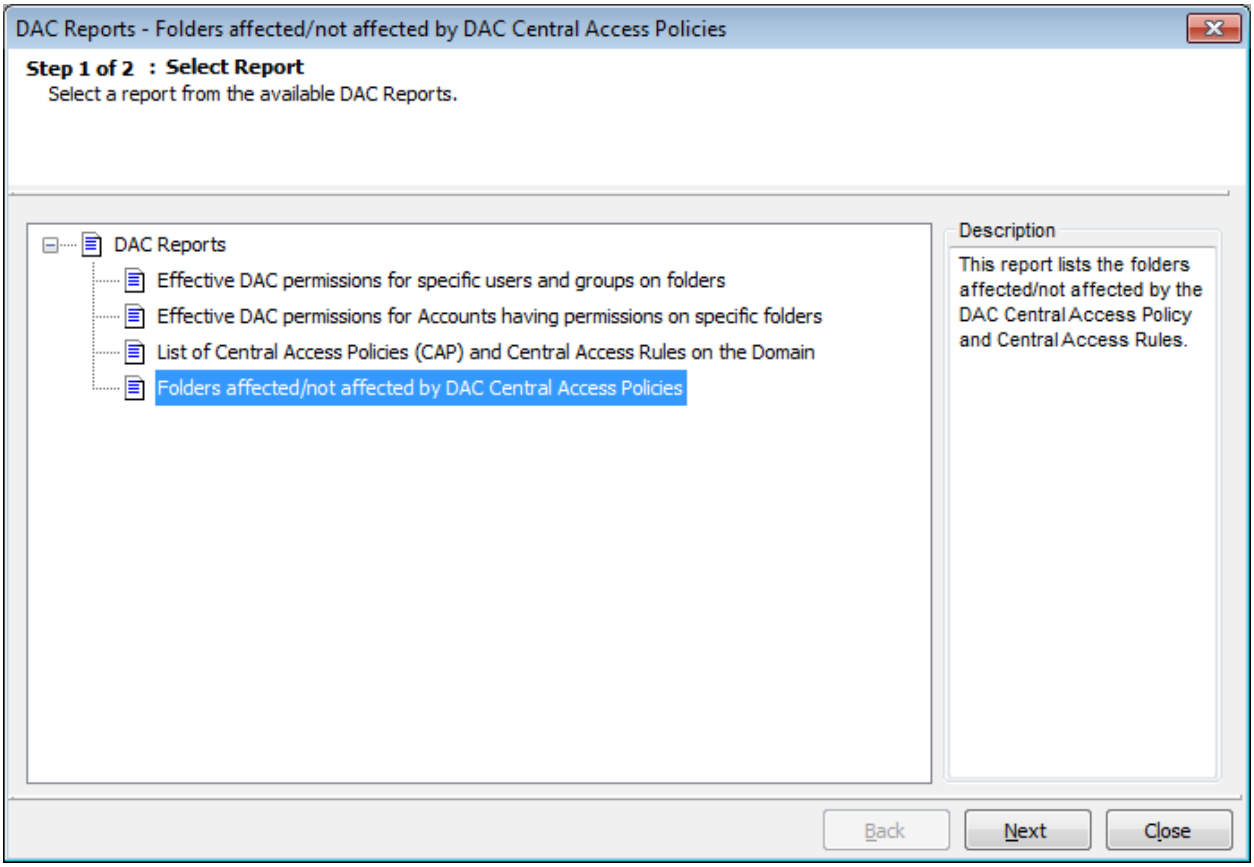
button.

The DAC Reports window with the list of reports will be displayed as shown below:

Step 1: Report Selection

Select the report to be generated. Only one report can be generated at a time.

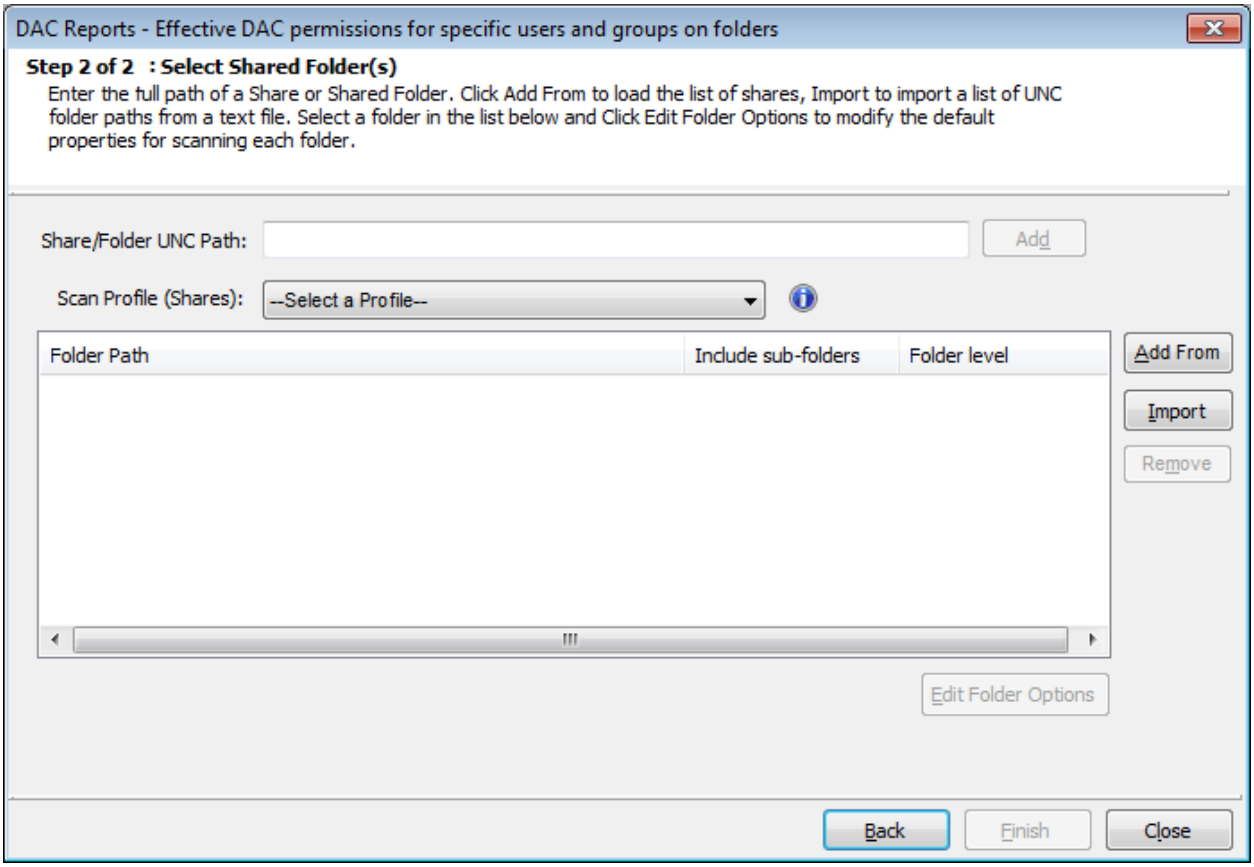

DAC Reports
Step 1 of 3 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
Select a report from the available DAC Reports.
Back
Next
Close


DAC Reports - Folders affected/not affected by DAC Central Access Policies
Step 1 of 2 : Select Report
Select a report from the available DAC Reports.
DAC Reports
Effective DAC permissions for specific users and groups on folders
Effective DAC permissions for Accounts having permissions on specific folders
List of Central Access Policies (CAP) and Central Access Rules on the Domain
Folders affected/not affected by DAC Central Access Policies
Description
This report lists the folders affected/not affected by the DAC Central Access Policy and Central Access Rules.
Back
Next
Close

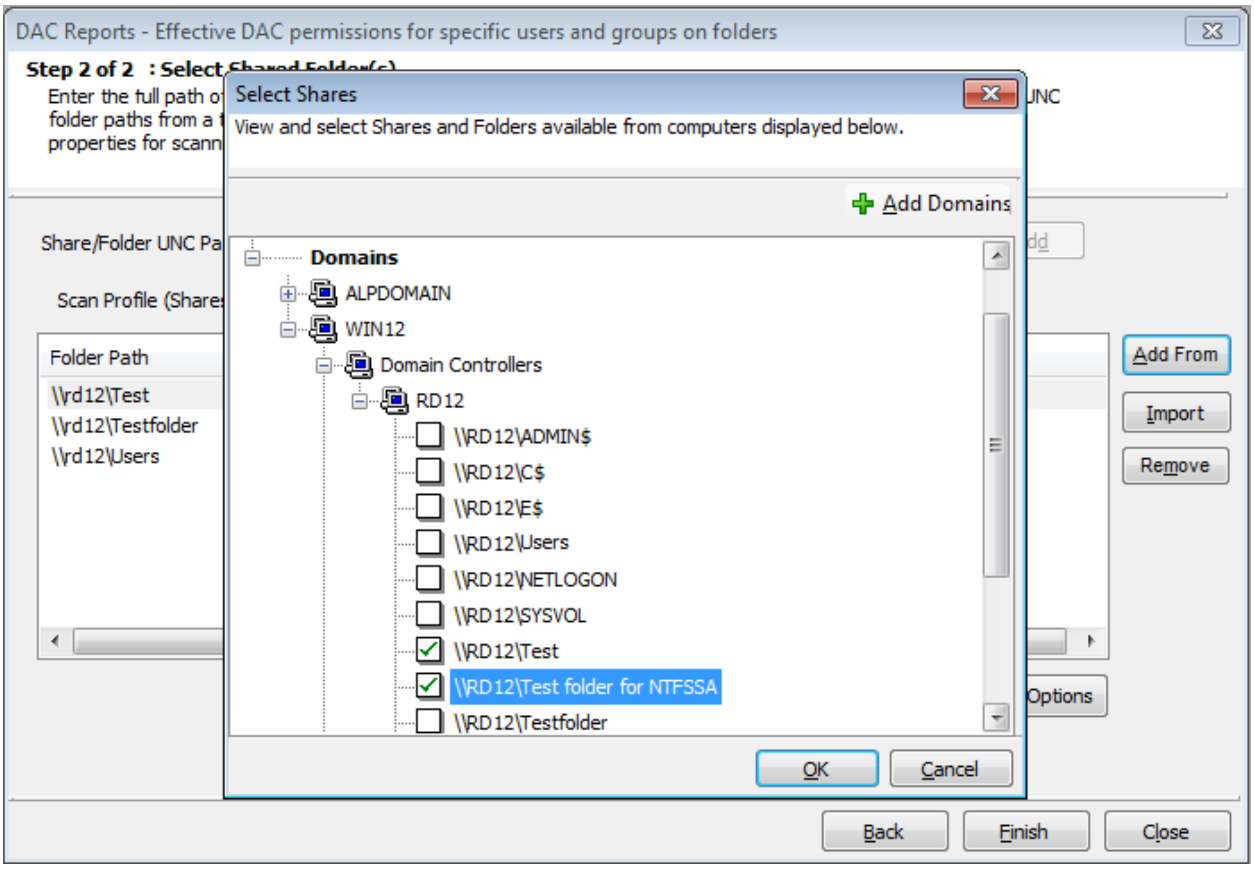
Click **Next** to proceed to the next step.

Step 2: Select shared folders

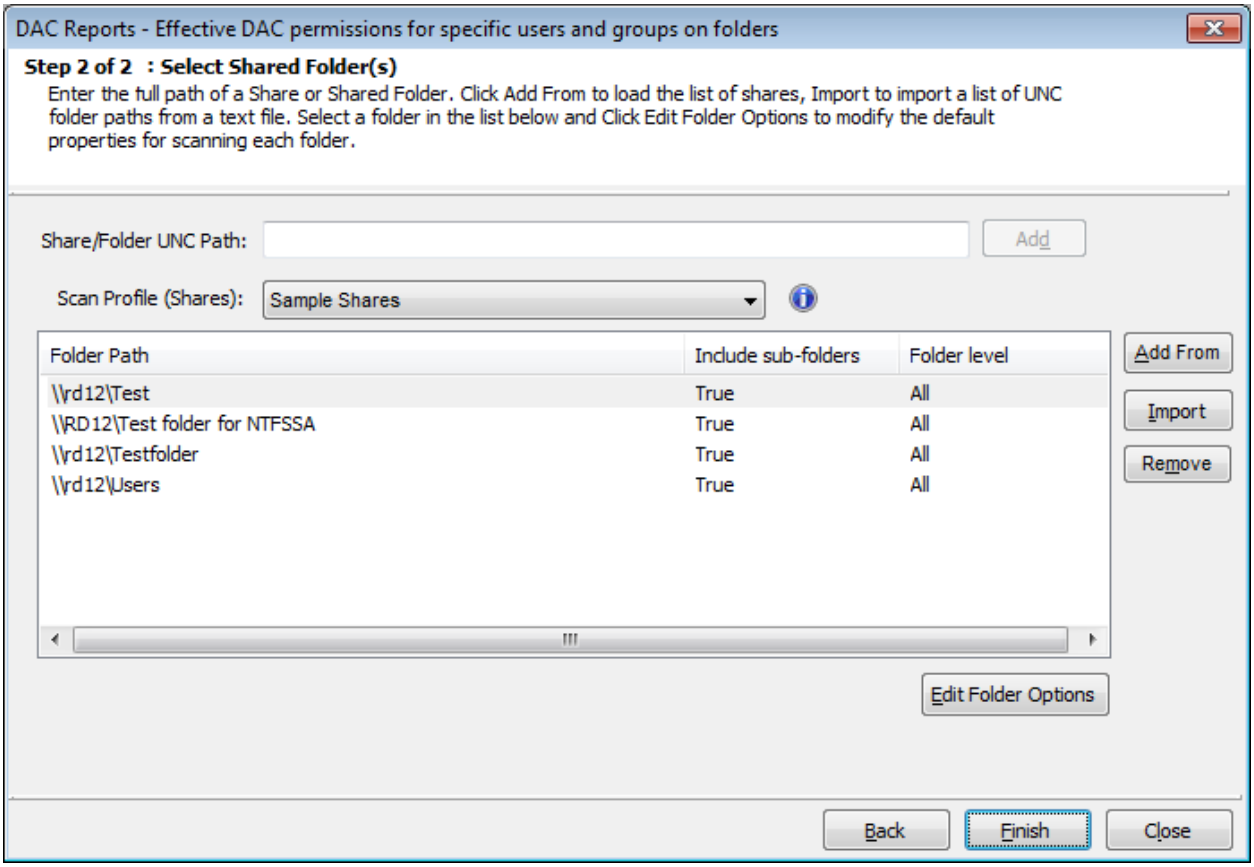
Select shared folder(s) by using any of the input options displayed.


DAC Reports - Effective DAC permissions for specific users and groups on folders
Step 2 of 2 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Edit Folder Options
Back
Finish
Close

- Click the option **Add From**
- Select one or more servers to enumerate its shared folders.

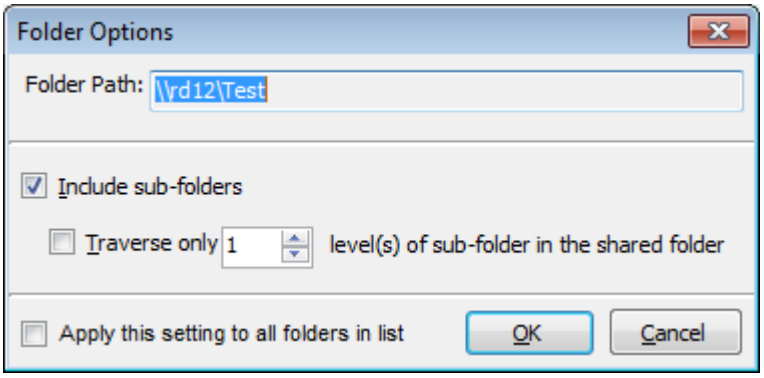


- Use **Select a Profile** option to use the shares added in the profile.



You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

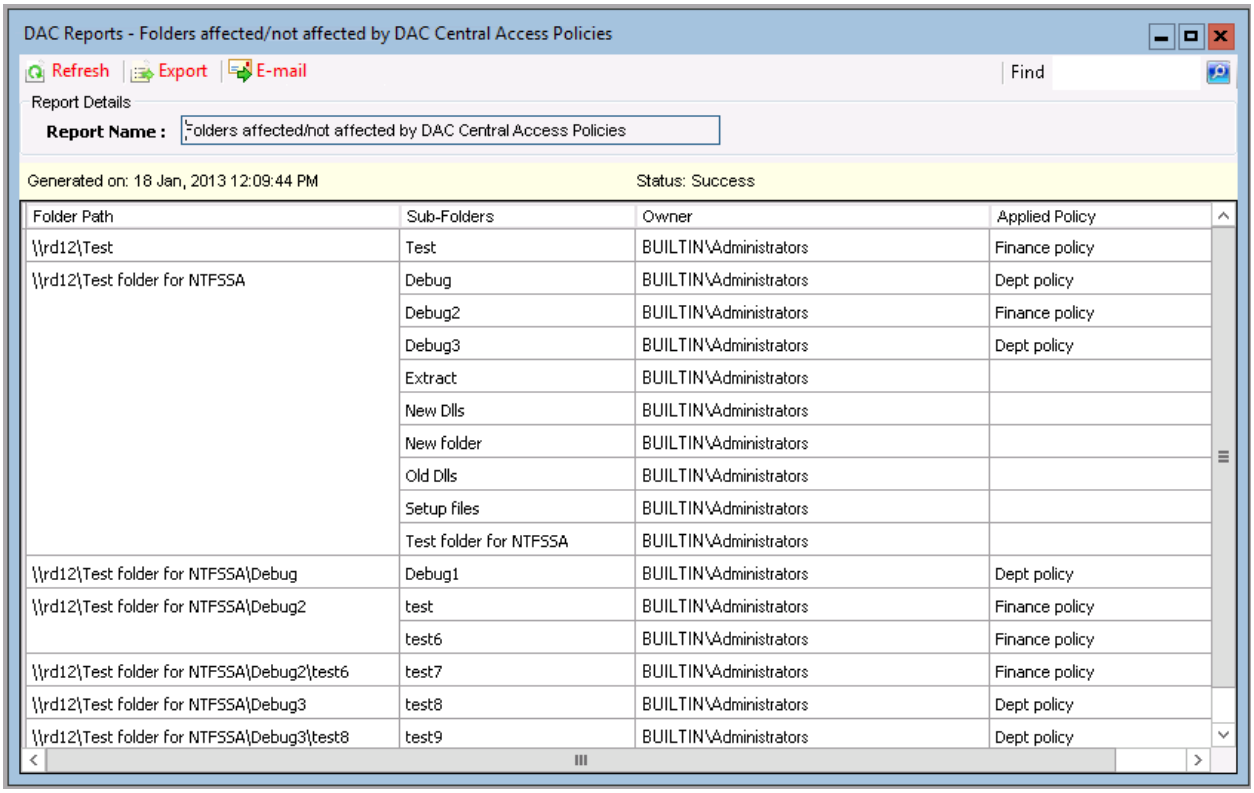
NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to proceed.

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



Folder Path	Sub-Folders	Owner	Applied Policy
\\rd12\Test	Test	BUILTIN\Administrators	Finance policy
\\rd12\Test folder for NTFSSA	Debug	BUILTIN\Administrators	Dept policy
	Debug2	BUILTIN\Administrators	Finance policy
	Debug3	BUILTIN\Administrators	Dept policy
	Extract	BUILTIN\Administrators	
	New Dlls	BUILTIN\Administrators	
	New folder	BUILTIN\Administrators	
	Old Dlls	BUILTIN\Administrators	
	Setup files	BUILTIN\Administrators	
	Test folder for NTFSSA	BUILTIN\Administrators	
\\rd12\Test folder for NTFSSA\Debug	Debug1	BUILTIN\Administrators	Dept policy
\\rd12\Test folder for NTFSSA\Debug2	test	BUILTIN\Administrators	Finance policy
	test6	BUILTIN\Administrators	Finance policy
\\rd12\Test folder for NTFSSA\Debug2\test6	test7	BUILTIN\Administrators	Finance policy
\\rd12\Test folder for NTFSSA\Debug3	test8	BUILTIN\Administrators	Dept policy
\\rd12\Test folder for NTFSSA\Debug3\test8	test9	BUILTIN\Administrators	Dept policy

Security Viewer

How to view the permissions for shares and local drives?

How to enumerate shared folders / files?

How to view the permissions for shares and local drives?

The **Security Viewer** feature allows you to view entire file system permissions. You can use many options to view the permissions of shares. With the option Local Drives you can view the permissions of the local system folders and files. With the option Domain you can view permissions of the shared folder(s)/file(s) in the entire network.

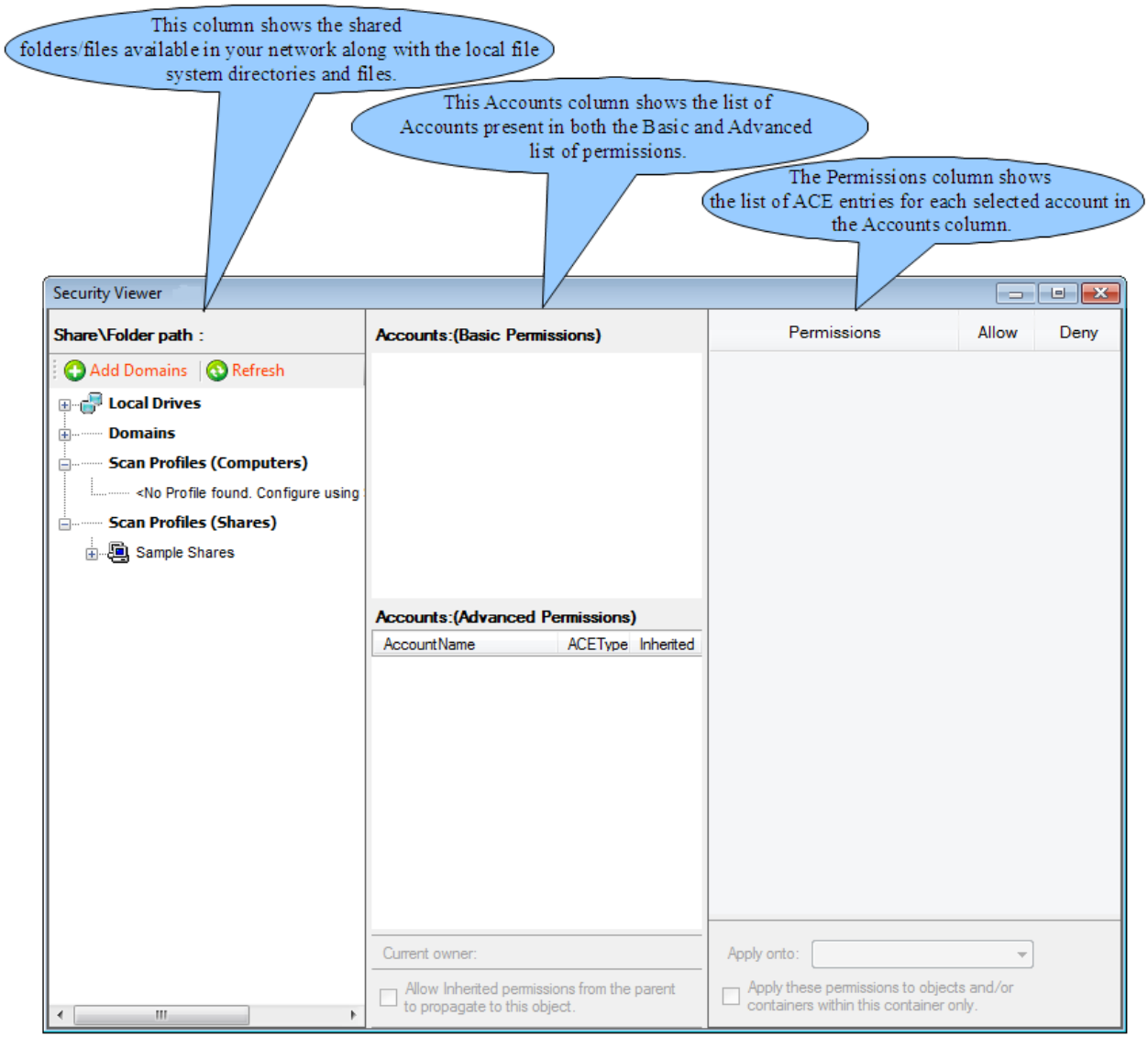
Click on

button.

The Security Viewer window will be displayed as shown below:

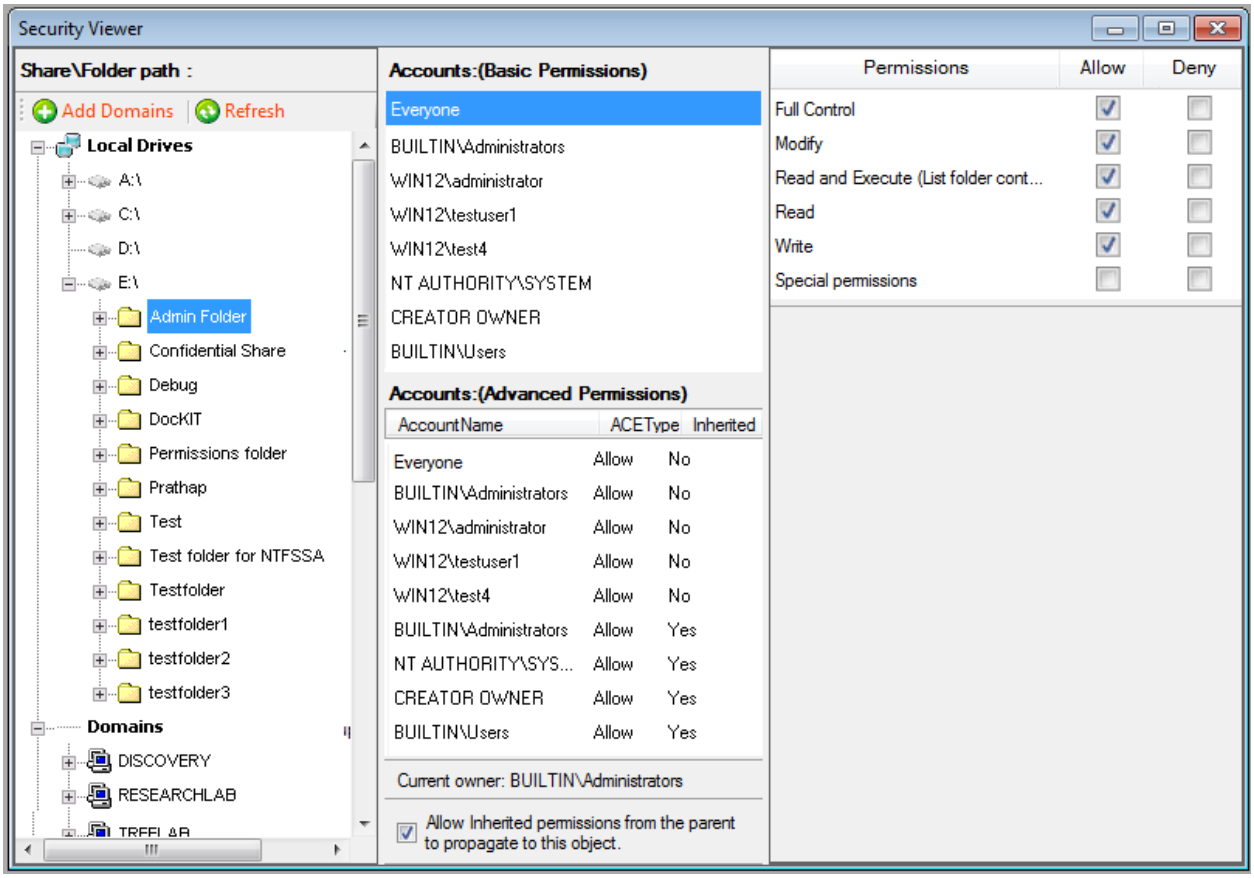
Step 1: Select folder/file path

Select folder/file path by using an option below.


This column shows the shared folders/files available in your network along with the local file system directories and files.
This Accounts column shows the list of Accounts present in both the Basic and Advanced list of permissions.
The Permissions column shows the list of ACE entries for each selected account in the Accounts column.
Security Viewer
Share\Folder path :
Add Domains
Refresh
Local Drives
Domains
Scan Profiles (Computers)
<No Profile found. Configure using
Scan Profiles (Shares)
Sample Shares
Accounts:(Basic Permissions)
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
Permissions
Allow
Deny
Current owner:
Allow Inherited permissions from the parent to propagate to this object.
Apply onto:
Apply these permissions to objects and/or containers within this container only.

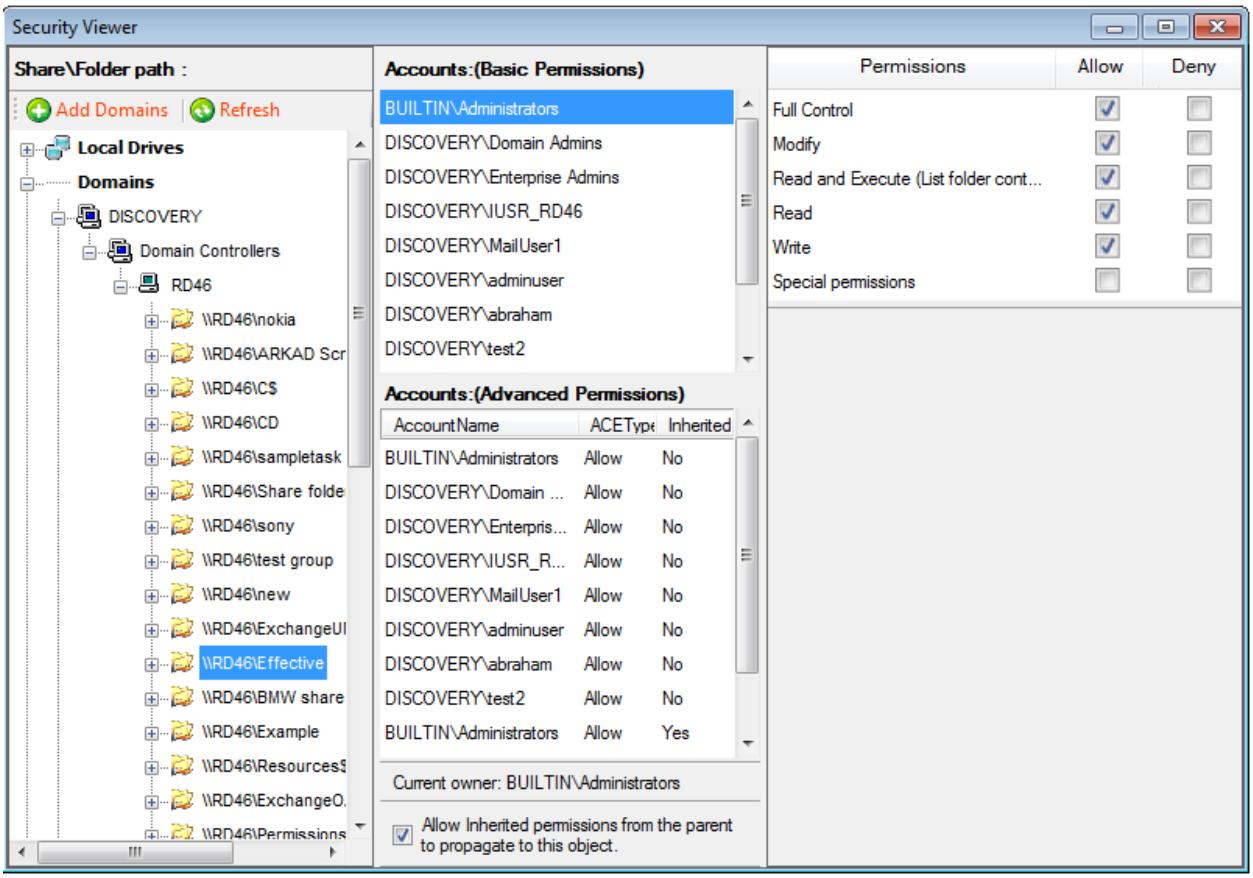
Select Local Drives and follow the steps below.

- Select and traverse one or more directory to enumerate its subfolders and files.
- Select a directory or subfolder/file path.



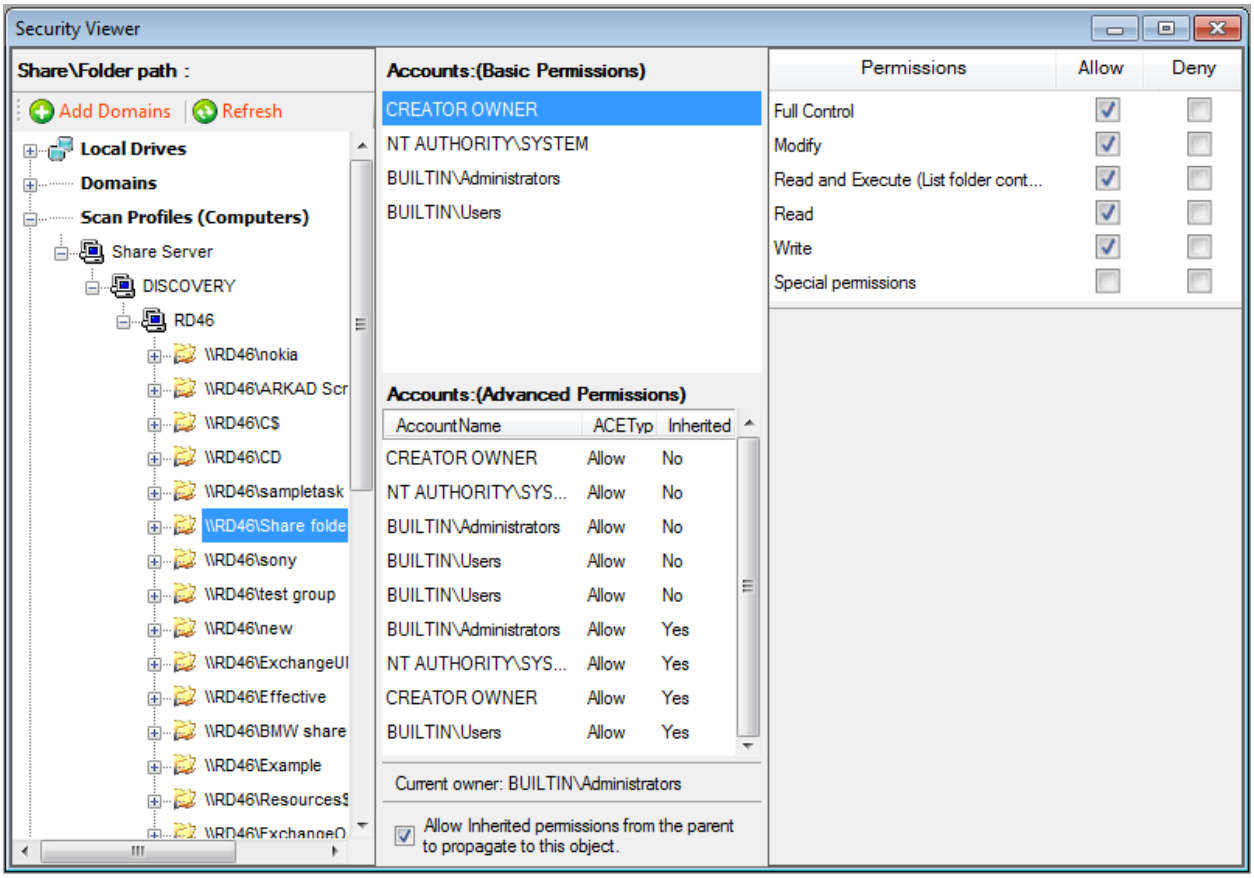
Select **Domains** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file path.
- Select a shared folder/file path.



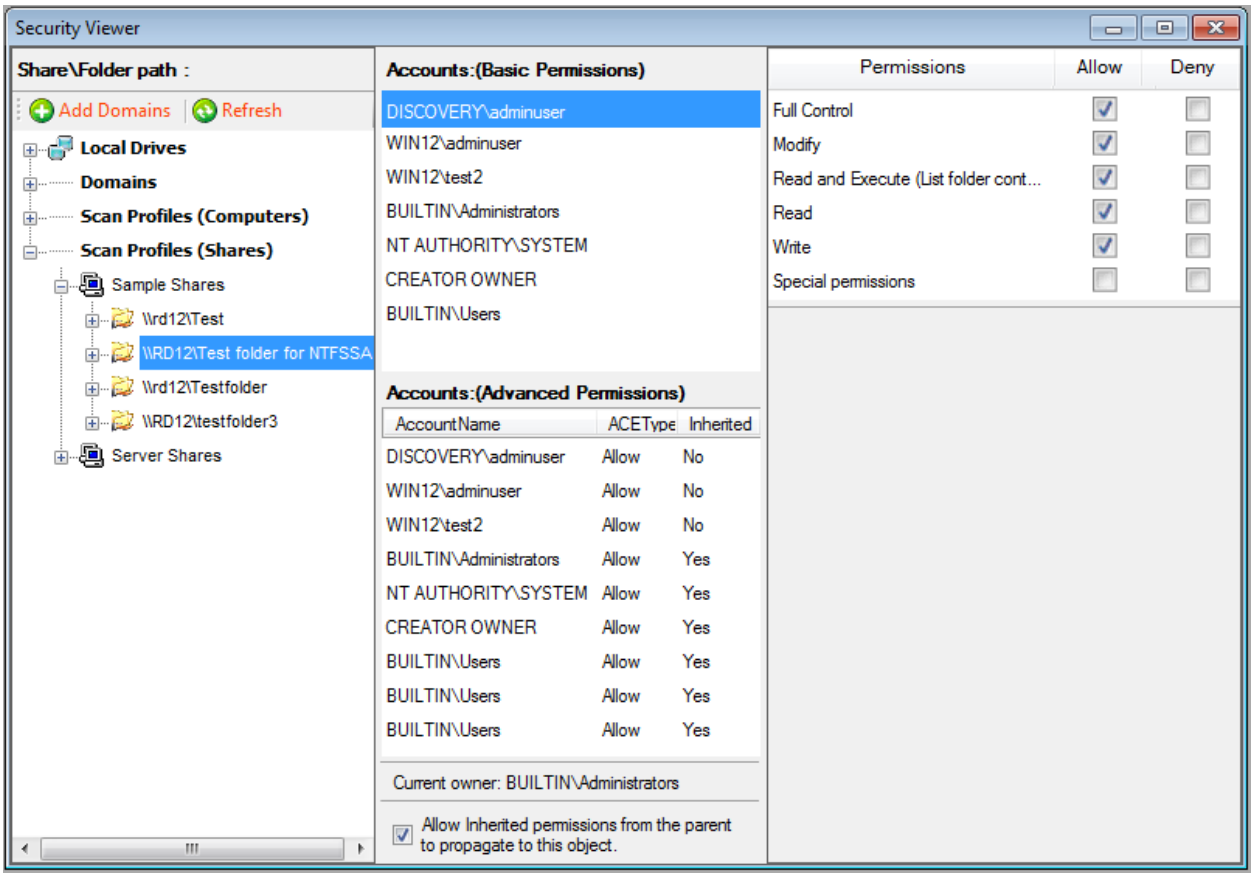
Select **Scan Profiles (Computers)** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file.
- Select a shared folder/file path.



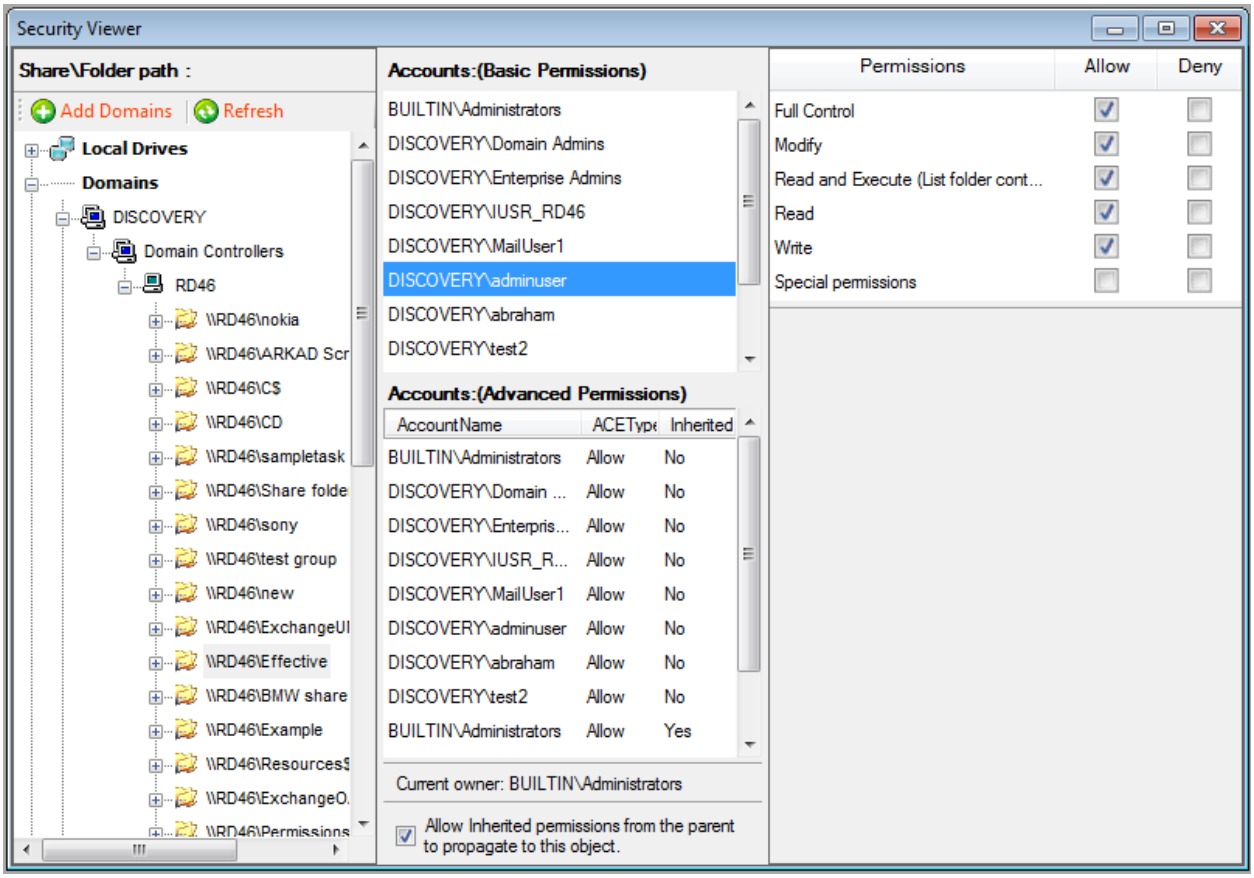
Select **Scan Profiles (Shares)** and follow the steps below.

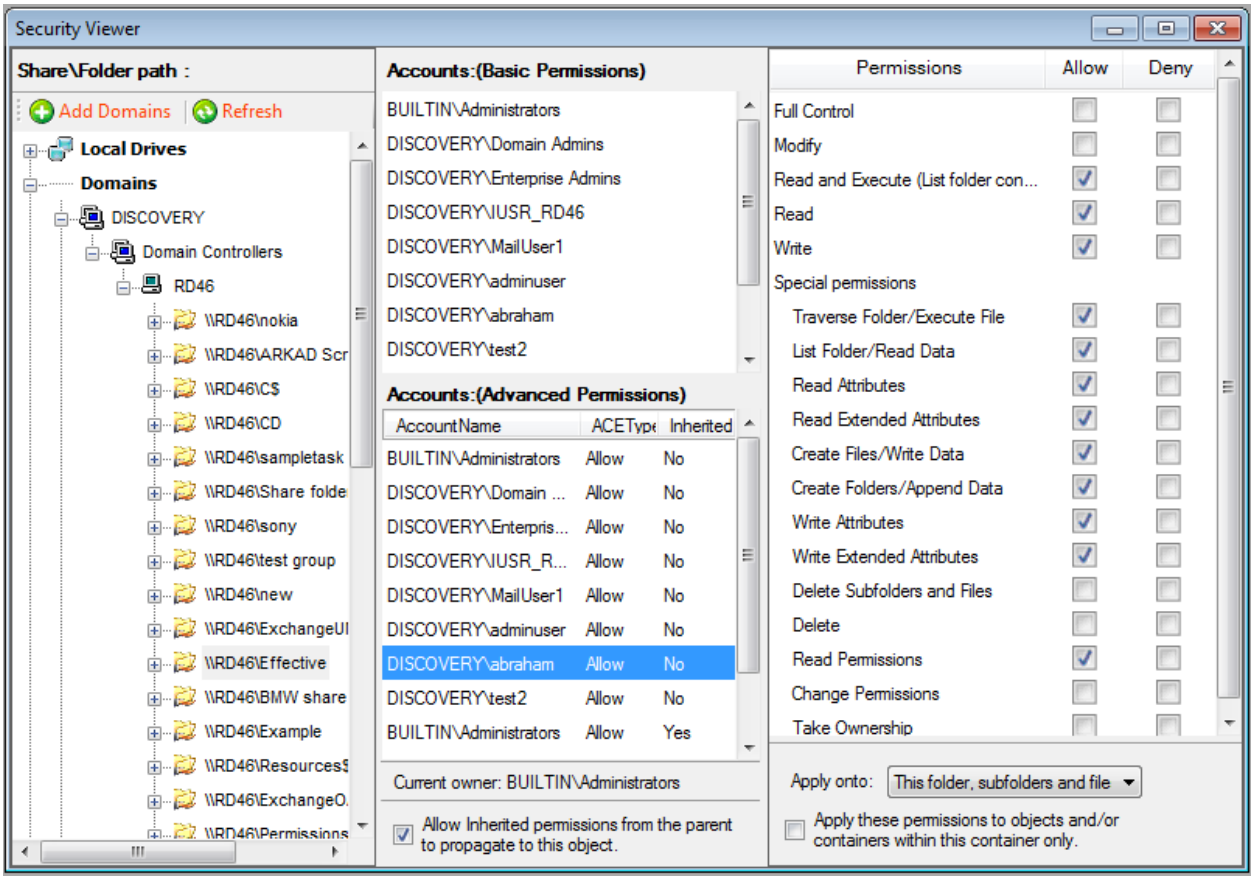
- Select Shares profile and enumerate its shared folder(s)/file(s) list.
- Select a shared folder/file path.


Security Viewer
Share\Folder path :
Add Domains
Refresh
Local Drives
Domains
Scan Profiles (Computers)
Scan Profiles (Shares)
Sample Shares
\\rd12\Test
\\RD12\Test folder for NTFSSA
\\rd12\Testfolder
\\RD12\testfolder3
Server Shares
Accounts:(Basic Permissions)
DISCOVERY\adminuser
WIN12\adminuser
WIN12\test2
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
CREATOR OWNER
BUILTIN\Users
Permissions
Allow
Deny
Full Control
Modify
Read and Execute (List folder cont...
Read
Write
Special permissions
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
DISCOVERY\adminuser Allow No
WIN12\adminuser Allow No
WIN12\test2 Allow No
BUILTIN\Administrators Allow Yes
NT AUTHORITY\SYSTEM Allow Yes
CREATOR OWNER Allow Yes
BUILTIN\Users Allow Yes
BUILTIN\Users Allow Yes
BUILTIN\Users Allow Yes
Current owner: BUILTIN\Administrators
Allow Inherited permissions from the parent to propagate to this object.

Step 2: Select an Account

Select an account from the Basic or Advanced permissions list. After selecting an account, permissions of that account would be shown in the last column as shown below.





You may also verify the inheritance from the parent object (allowed or blocked) to this current object by using the option "Allow inherited permissions from the parent to propagate this object". If this option is checked then the inheritance from the parent to this current object has been allowed, otherwise if unchecked, it has been blocked.

How to enumerate shared folders/files?

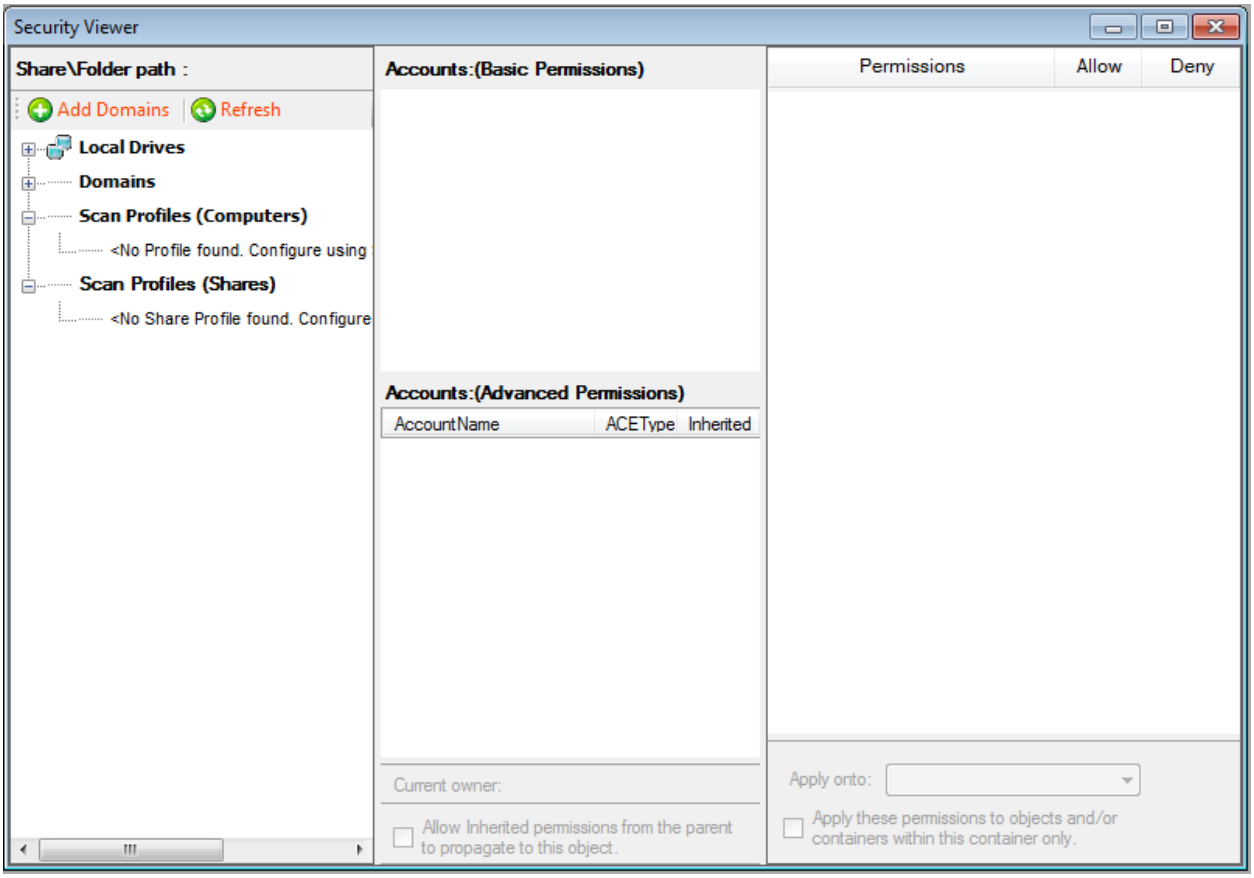
The **Security Viewer** feature allows many options to enumerate the shared folders/files in the entire network. You can also enumerate and view the folders and files in the local file system.

Click on

button.

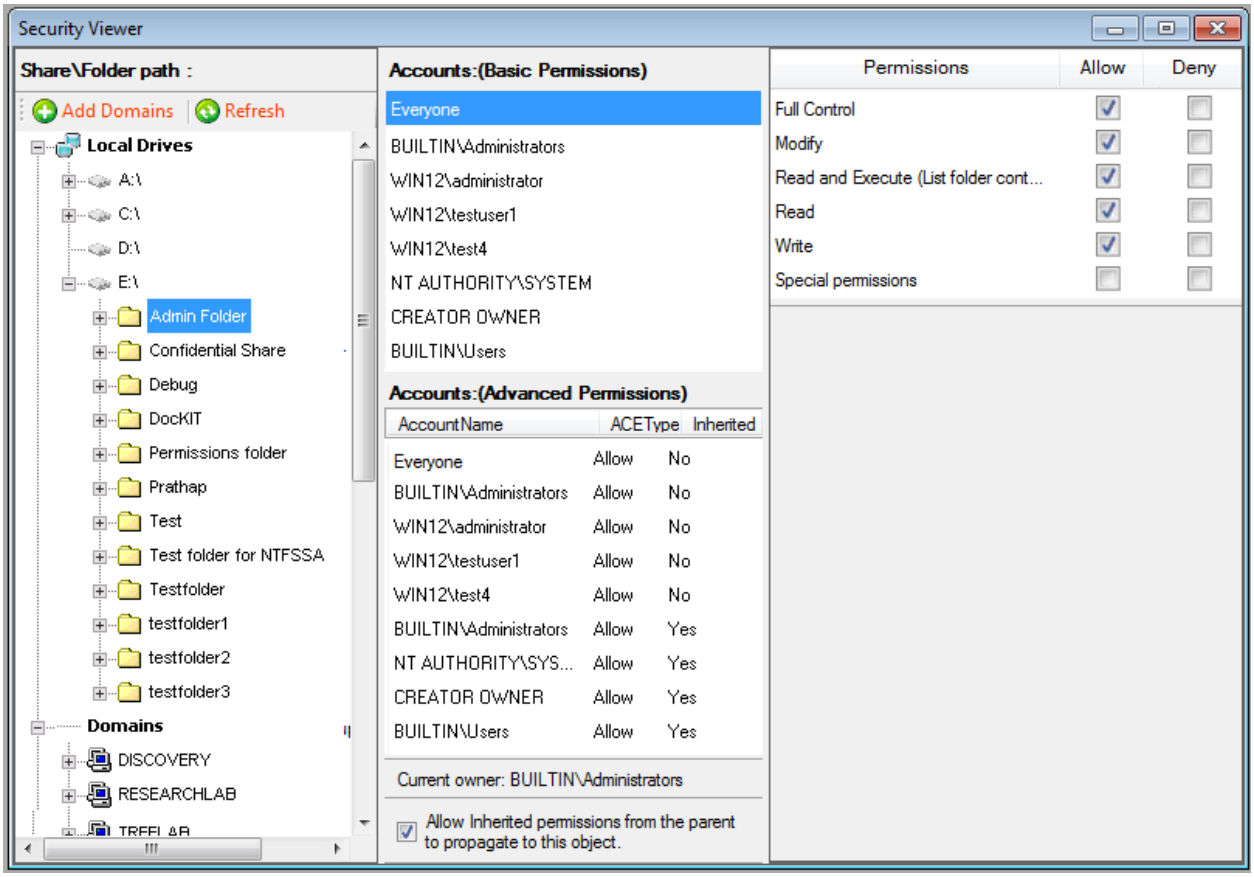
The **Security Viewer** window will be displayed as shown below. Here is the list of ways you can enumerate the shared folders/files in the network.

- Local Drives
- Domains
- Scan Profiles (Computers)
- Scan Profiles (Shares)



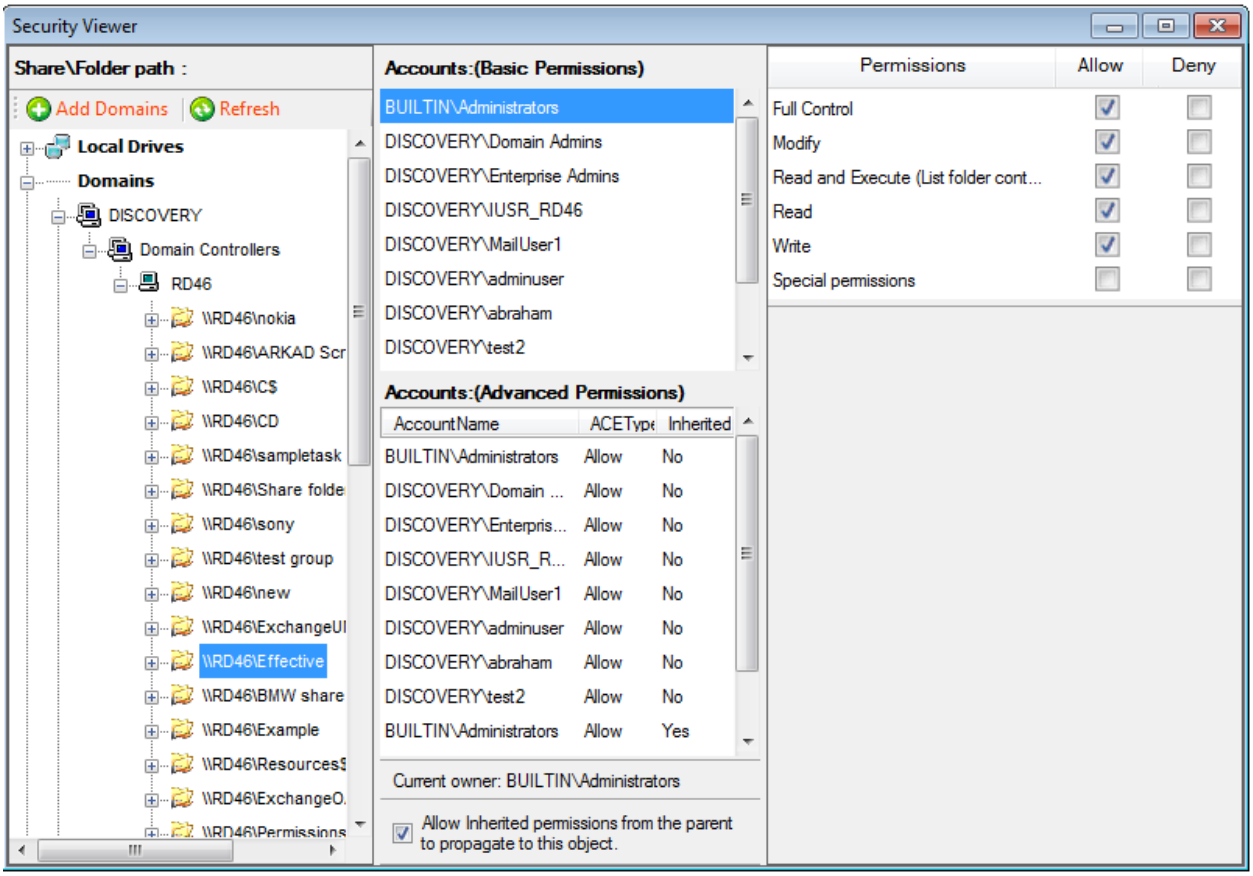
Select **Local Drives** and follow the steps below.

- Select and traverse one or more directory to enumerate its subfolders and files.
- Select a directory or subfolder/file path.



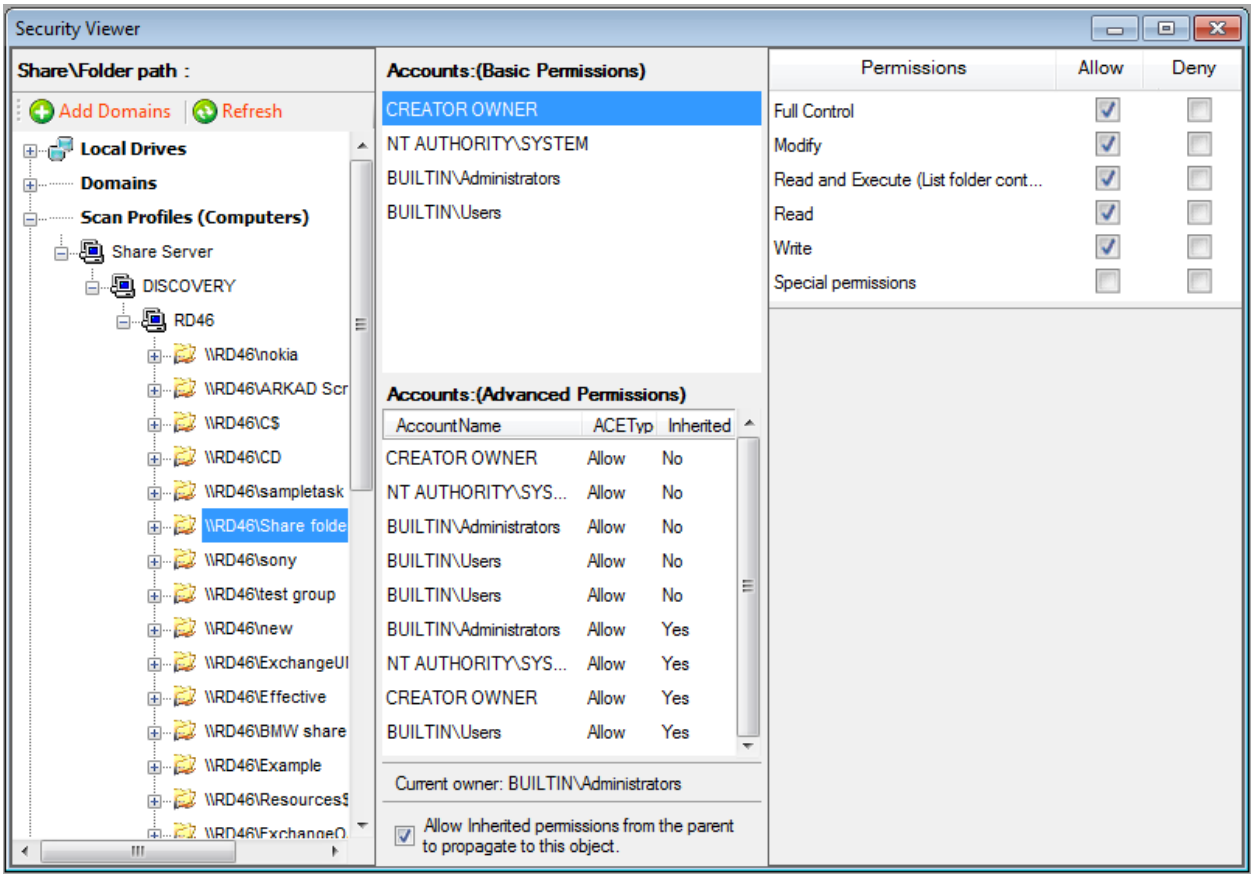
Select **Domains** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file path.
- Select a shared folder/file path.



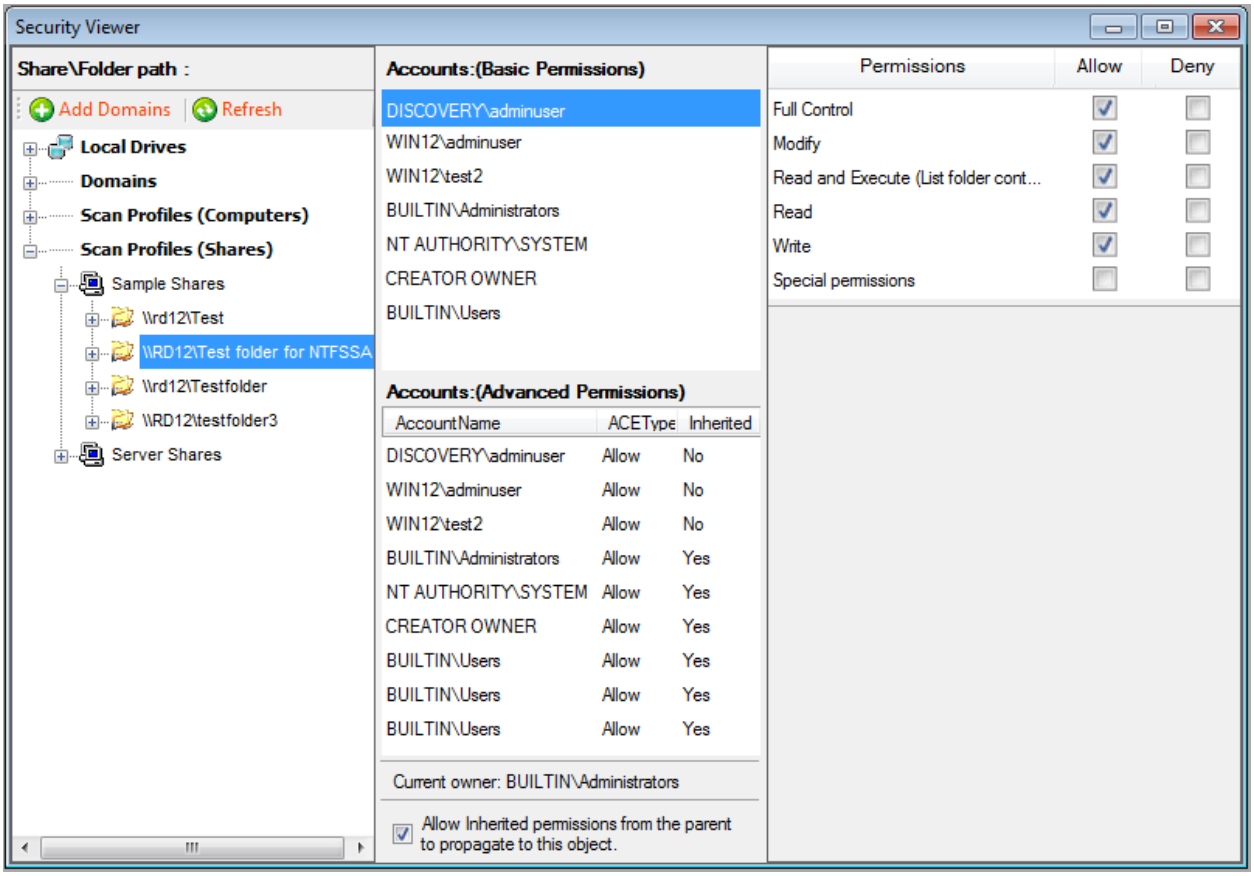
Select **Scan Profiles (Computers)** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file.
- Select a shared folder/file path.



Select **Scan Profiles (Shares)** and follow the steps below.

- Select shares profile and enumerate its shared folder(s)/file(s) list.
- Select a shared folder/file path.



Power Search

About Power Search

How to view Power Search Permissions (DACL) Reports?

How to view Power Search Auditing (SACL) Reports?

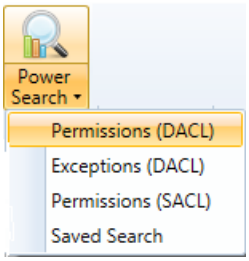
How to manage Power Search?

About Power Search

The Power Search feature lets you perform powerful, conditional Search queries of NTFS Permissions on Files and Folders. You may select specific permissions from the list of standard permissions and Advanced (special) permissions and run a query to determine who have these permissions on which folders and files. You may Save frequently used queries for reuse them later. Here are some examples of how you may make effective use of this feature:

1. Search on who has Full Control on which folders and files
2. Select a set of accounts and determine for which folders and files they have Full control access.
3. Determine which accounts have modify or delete permissions on critical files and folders.
4. Determine what type of permissions members of the Administrators group have on specific folders and files.
5. Determine where Inheritance from Parent folder has been explicitly removed.
6. Determine Accounts for which folders have explicit Allows or Denys set on them.

How to view Power Search Permissions (DACL) Reports?

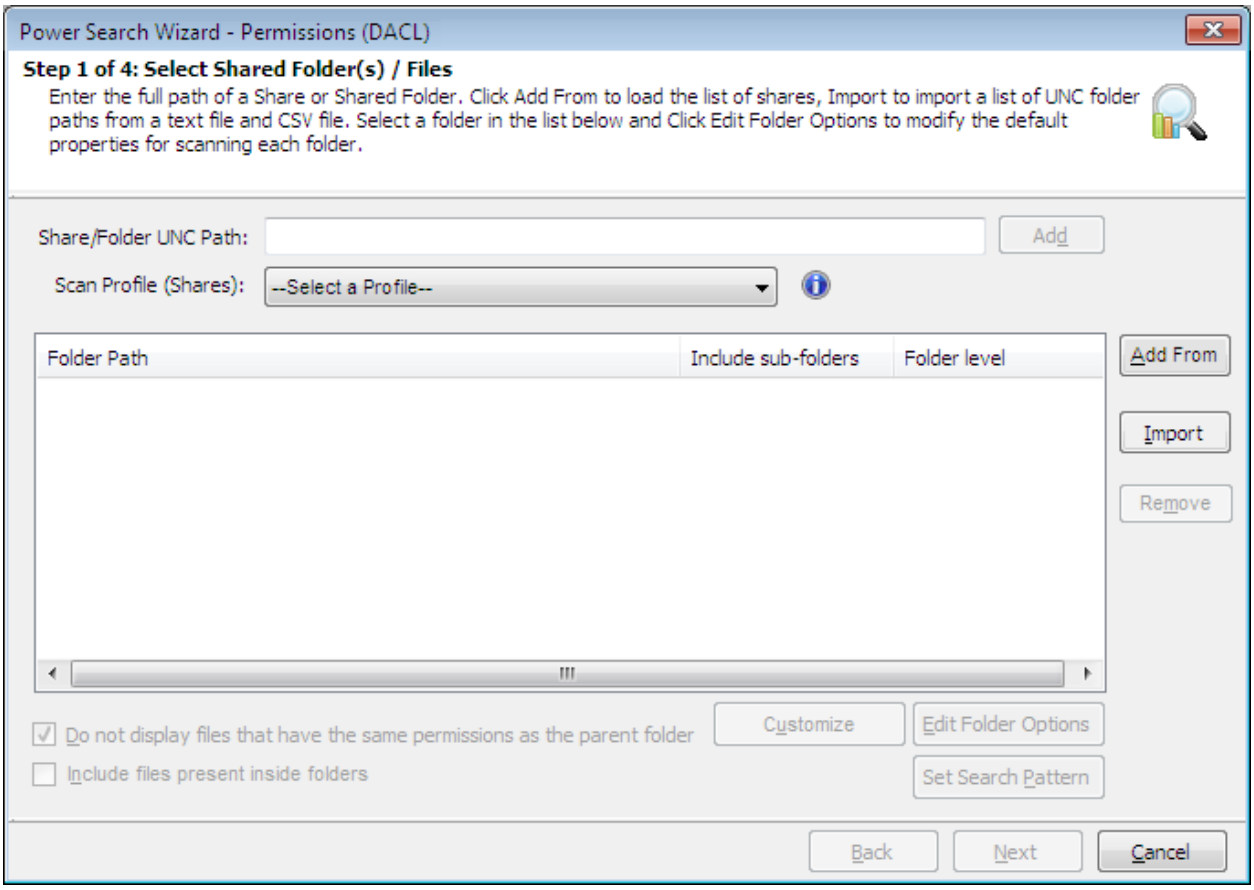


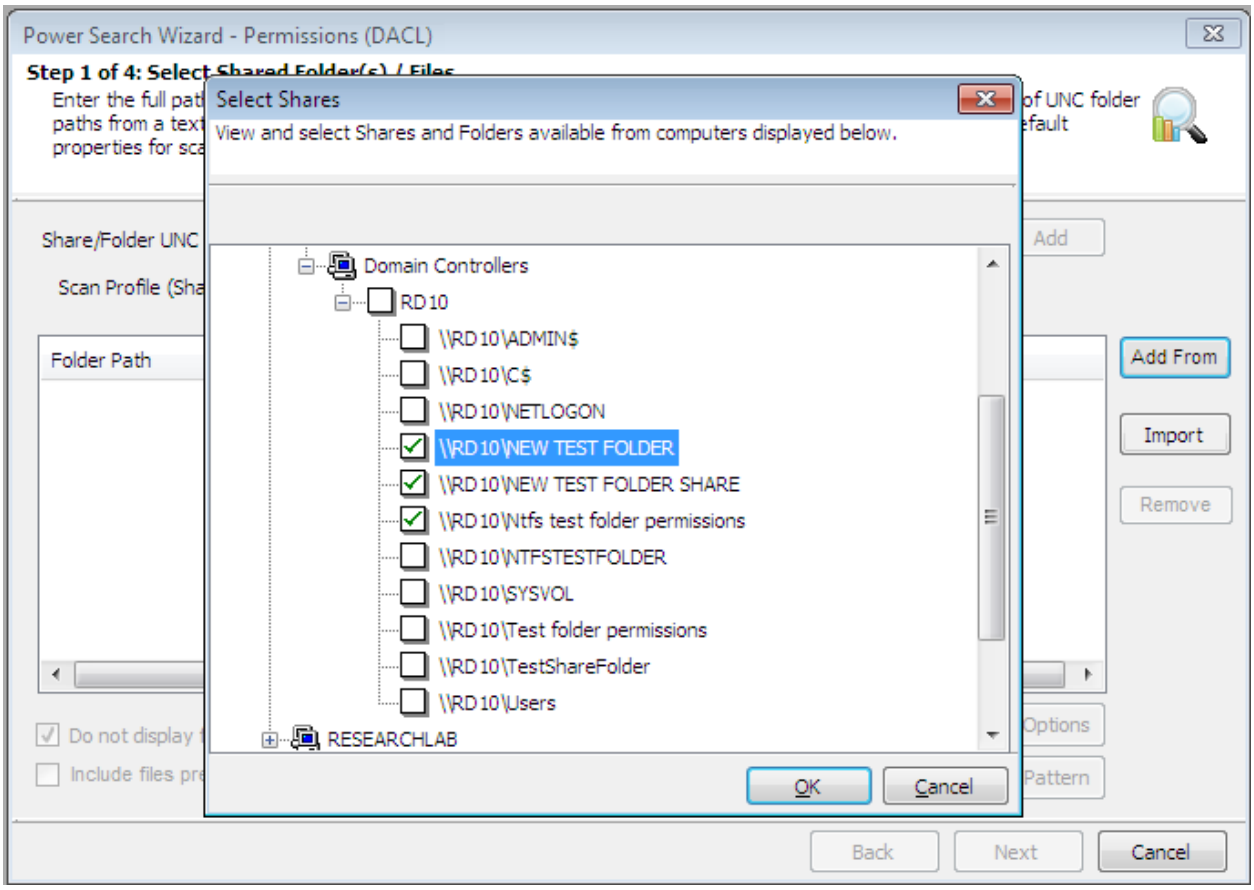
Click on button under Power Search.

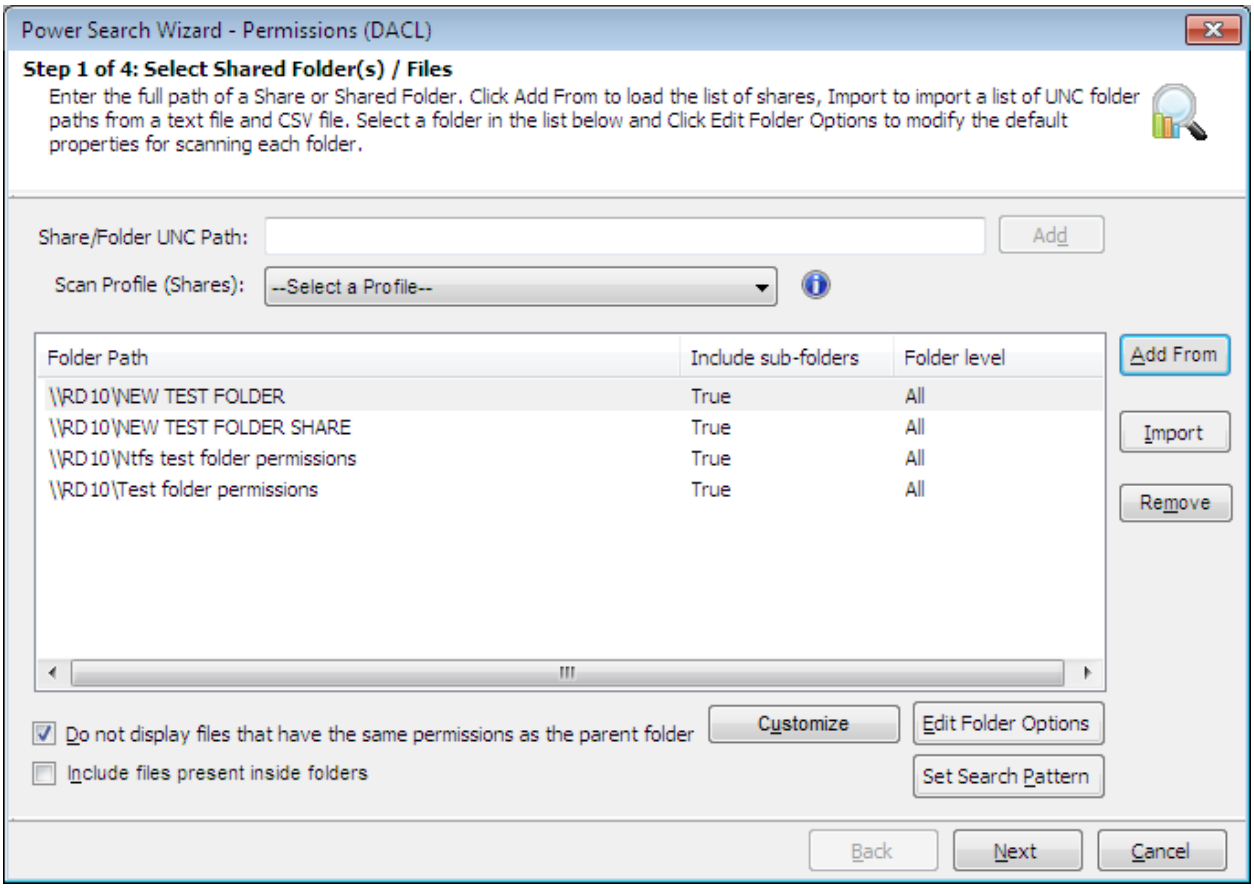
The Power Search window will be displayed as shown below:

Step 1: Select Shared Folder(s)/Files

Select one or more servers to enumerate its Shared Folder(s)/Files


Power Search Wizard - Permissions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel


Power Search Wizard - Permissions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full pat
paths from a text
properties for sca
of UNC folder
efault
Share/Folder UNC
Add
Scan Profile (Sha
Folder Path
Add From
Import
Remove
Do not display f
Include files pre
Options
Pattern
Back
Next
Cancel
Select Shares
View and select Shares and Folders available from computers displayed below.
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\Ntfs test folder permissions
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\Test folder permissions
\\RD10\TestShareFolder
\\RD10\Users
RESEARCHLAB
OK
Cancel

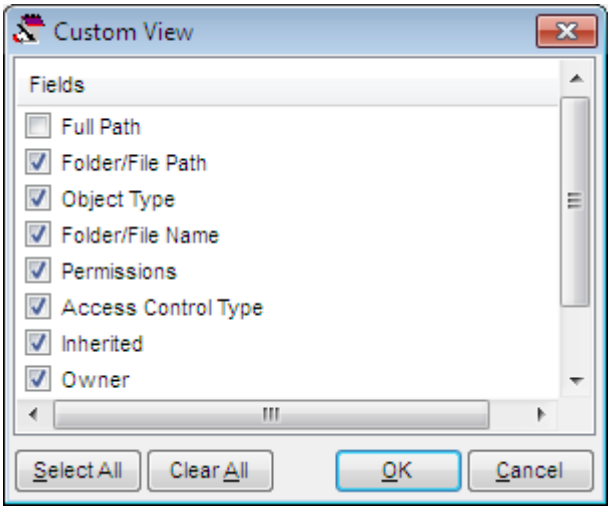

Power Search Wizard - Permissions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
\\RD10\Test folder permissions
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

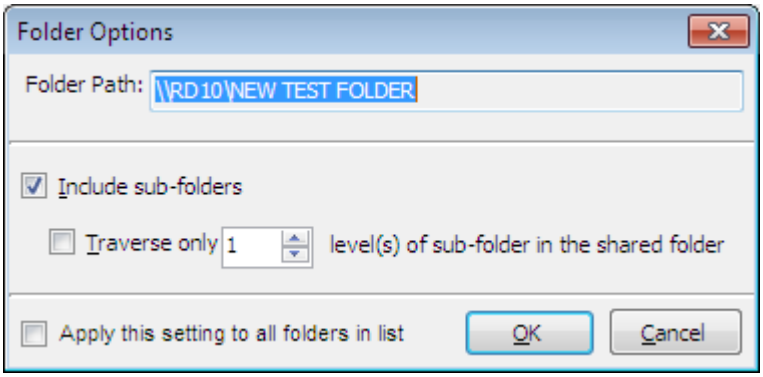
Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

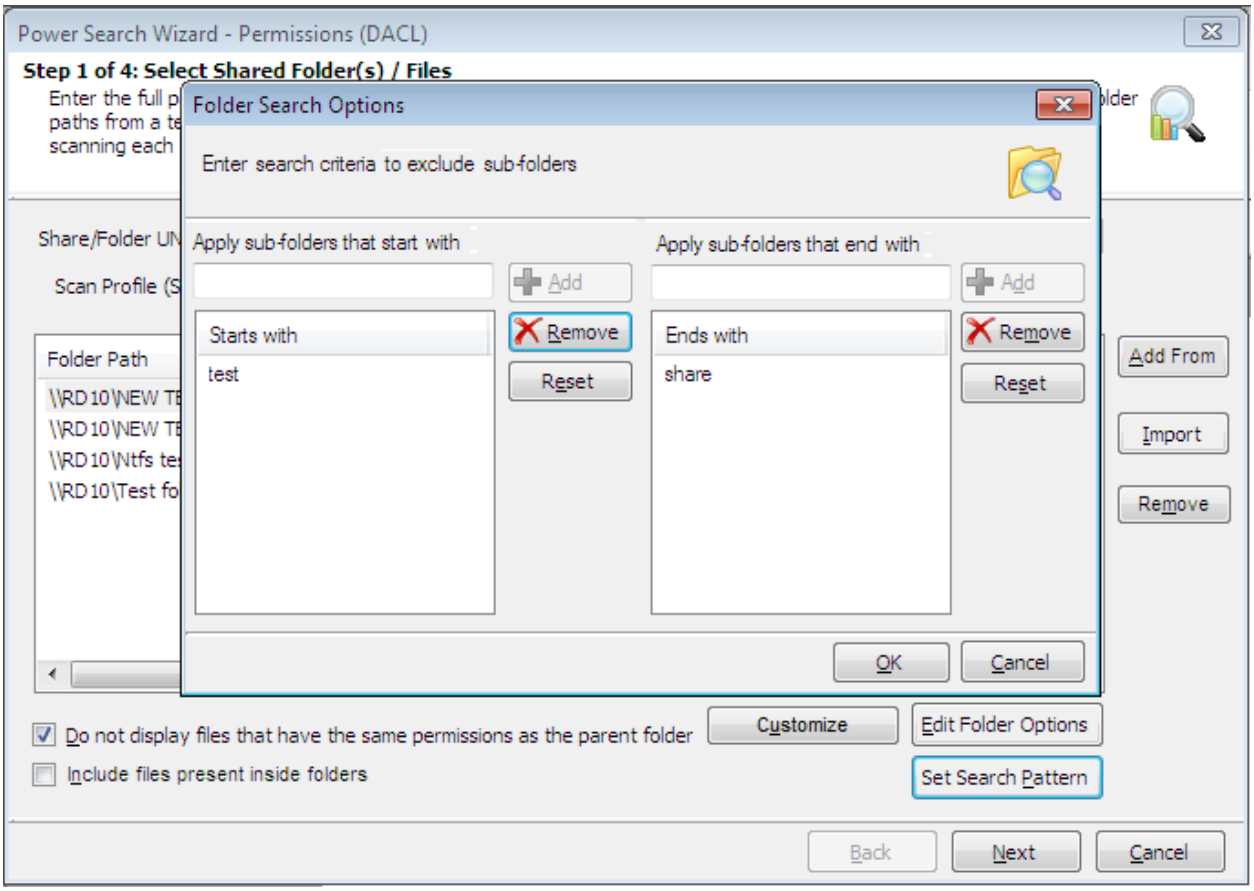
You can use Customize option to exclude some of the fields from the reports, as displayed below:



NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



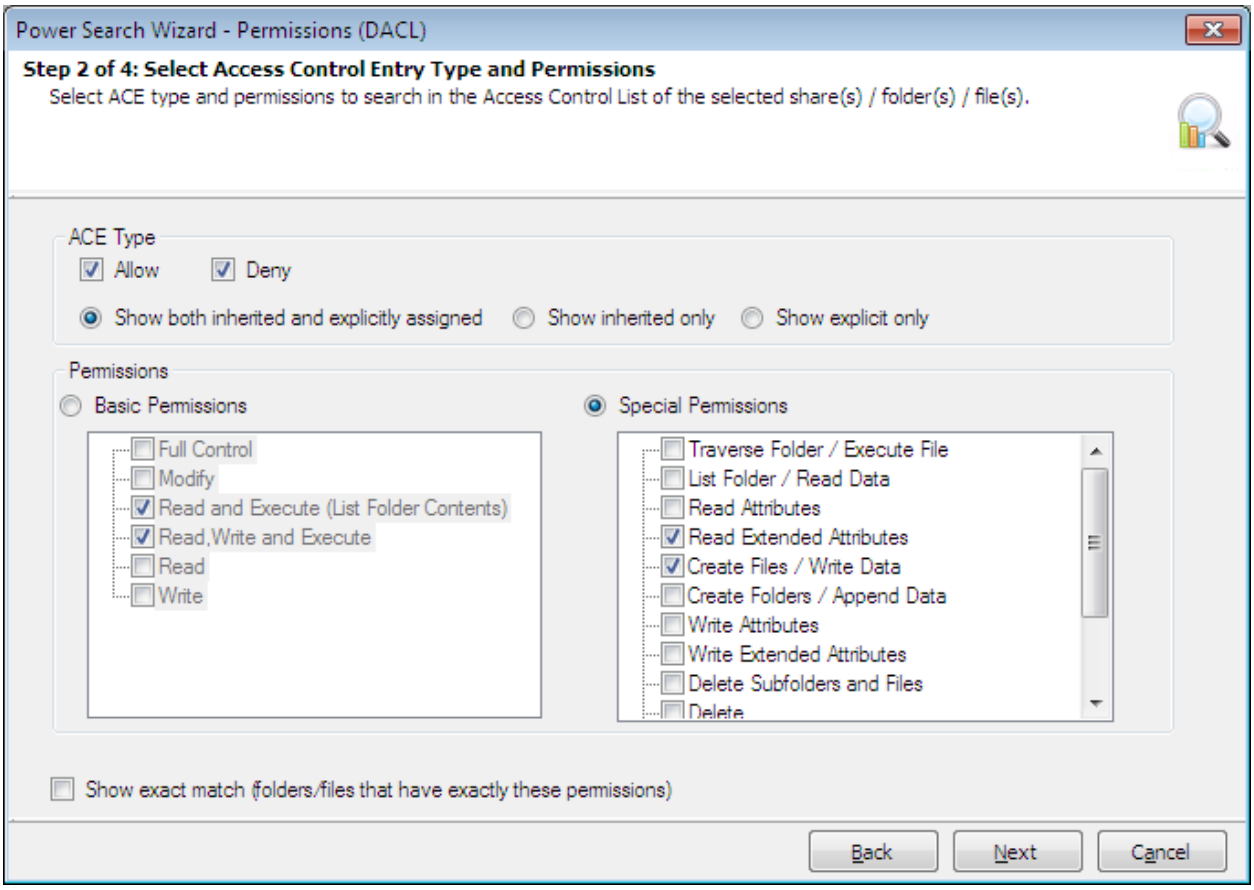
Use **Set Search Pattern** option to exclude sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example Folder name starts with test, Folder name ends with share.



Click **Next** to proceed to the next step.

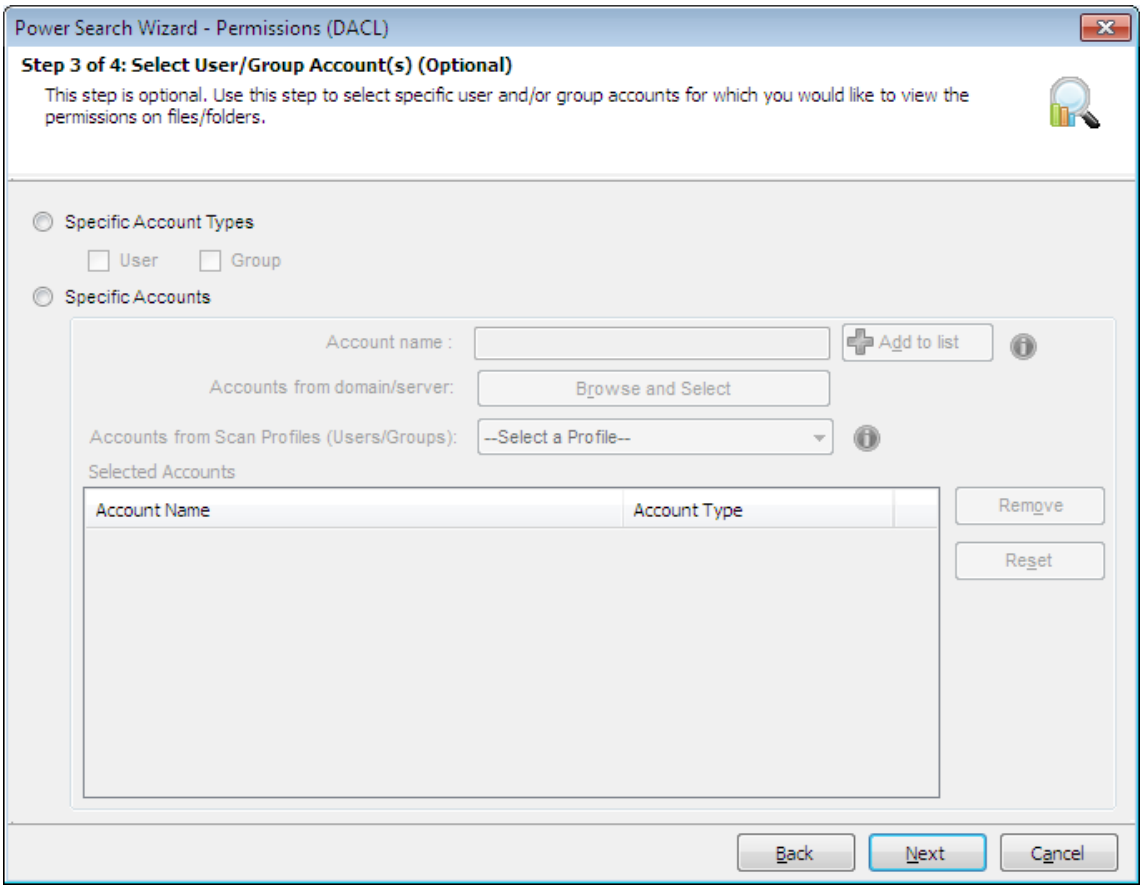
Step 2: Select Access Control Entry Type and Permissions

Select ACE Type and permissions to search in the Access Control List of the selected share(s) / folder(s) /files(s)

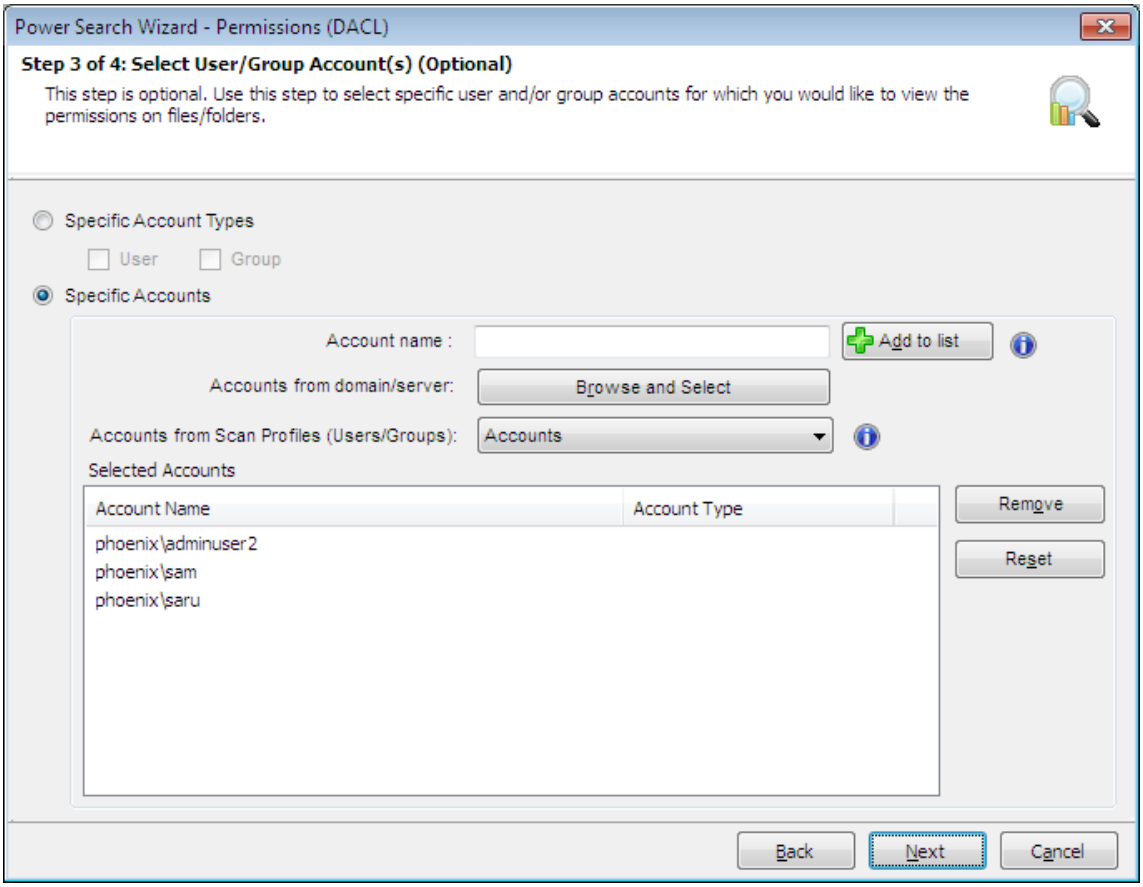


Step 3: User and/or Group Selection

1. **Specific Account Types**: Select user and/or group, for which you wish to run the search.
2. **Specific Accounts**: Select user and/or group accounts for which you would like to view the permissions for files/folders.



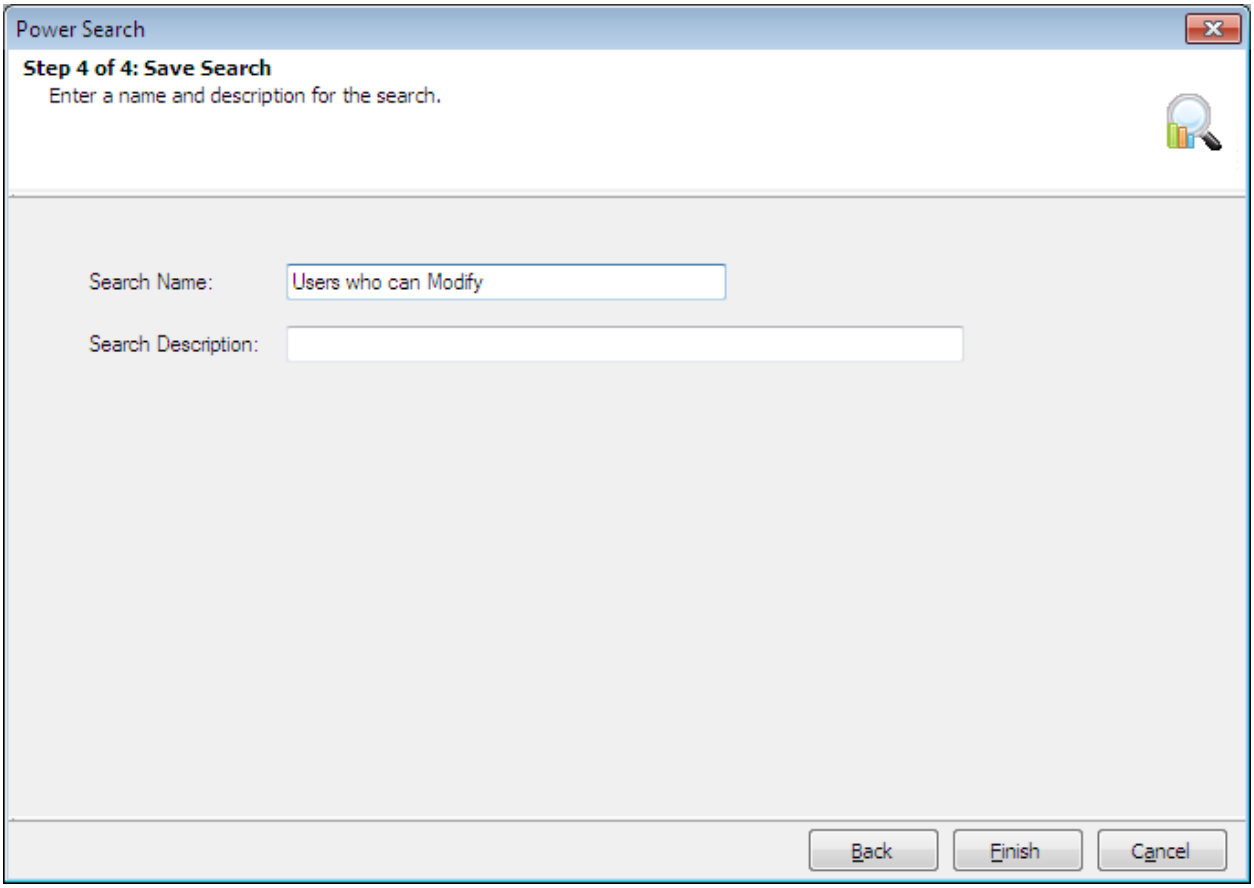
- Use Select a Scan Profile (Users/Groups) option to use the users and groups added in the profile.



- Click **Next** to proceed to the Next step.

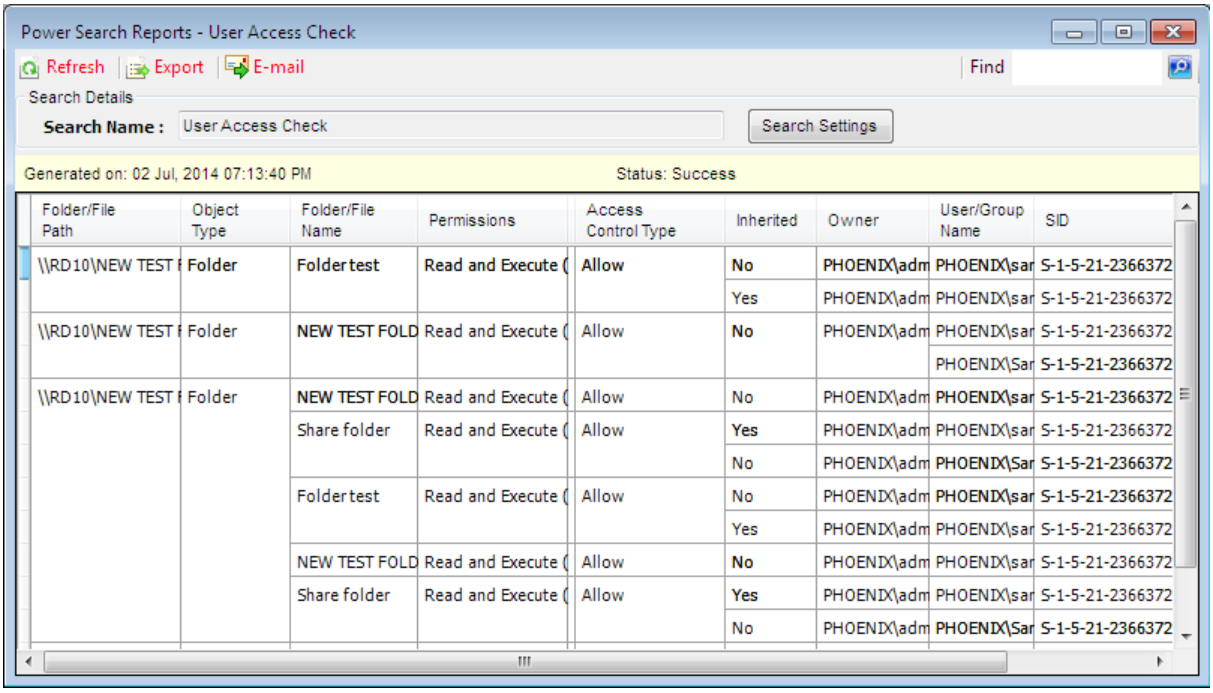
Step 4: Save Search

Enter a name and description for search.



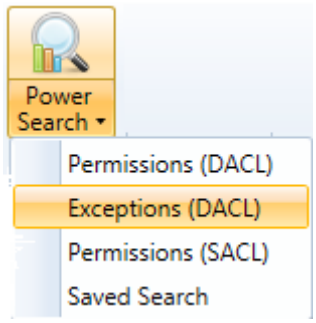
Click **Finish** to generate the power search report.

After the data collection process is complete, the report would be generated in a report window as shown below:



Folder/File Path	Object Type	Folder/File Name	Permissions	Access Control Type	Inherited	Owner	User/Group Name	SID
\\RD10\NEW TEST F	Folder	Folder test	Read and Execute (	Allow	No	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
					Yes	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
\\RD10\NEW TEST F	Folder	NEW TEST FOLD	Read and Execute (	Allow	No	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
							PHOENIX\Sar	S-1-5-21-2366372
\\RD10\NEW TEST F	Folder	NEW TEST FOLD	Read and Execute (	Allow	No	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
		Share folder	Read and Execute (	Allow	Yes	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
					No	PHOENIX\adm	PHOENIX\Sar	S-1-5-21-2366372
		Folder test	Read and Execute (	Allow	No	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
					Yes	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
		NEW TEST FOLD	Read and Execute (	Allow	No	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
		Share folder	Read and Execute (	Allow	Yes	PHOENIX\adm	PHOENIX\sar	S-1-5-21-2366372
					No	PHOENIX\adm	PHOENIX\Sar	S-1-5-21-2366372

How to view Power Search Exceptions (DACL) Reports?

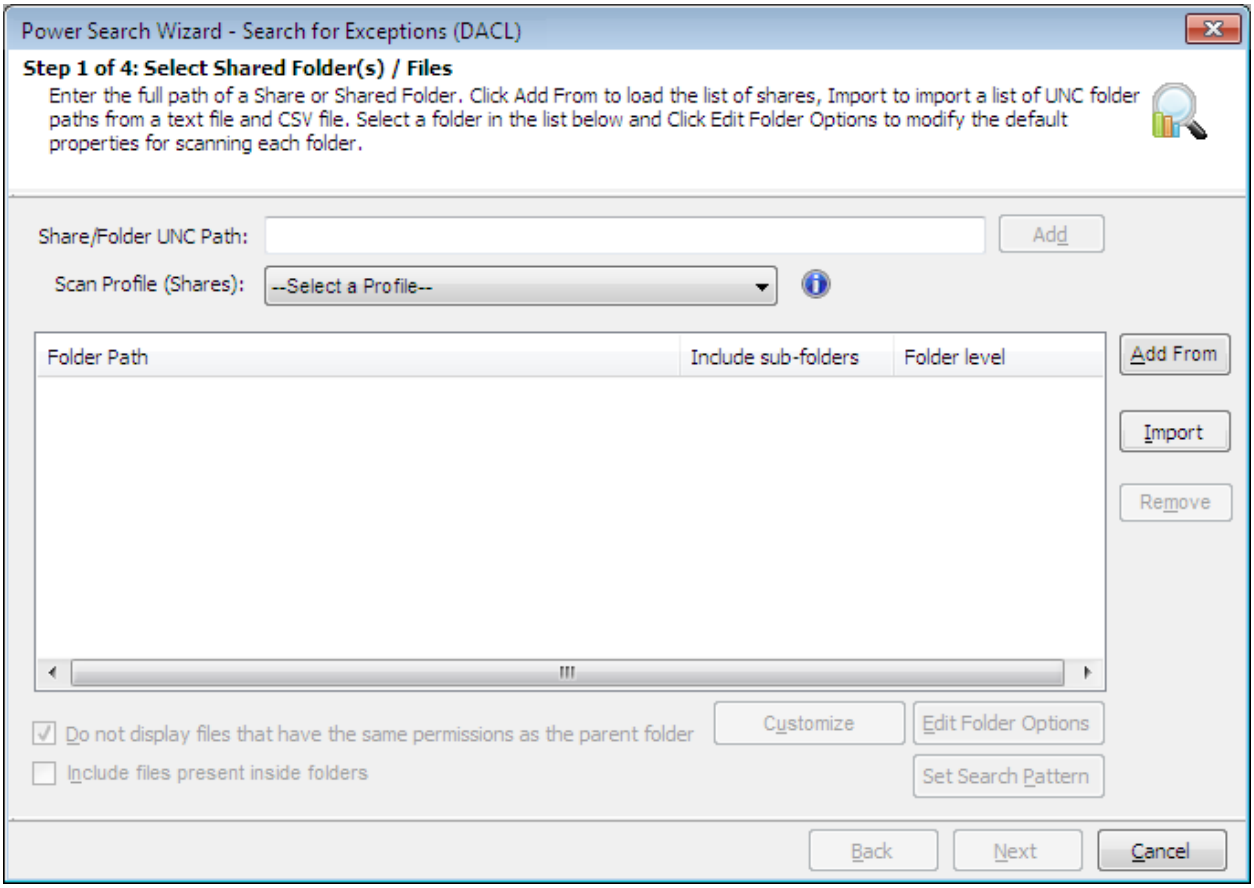
Click on 

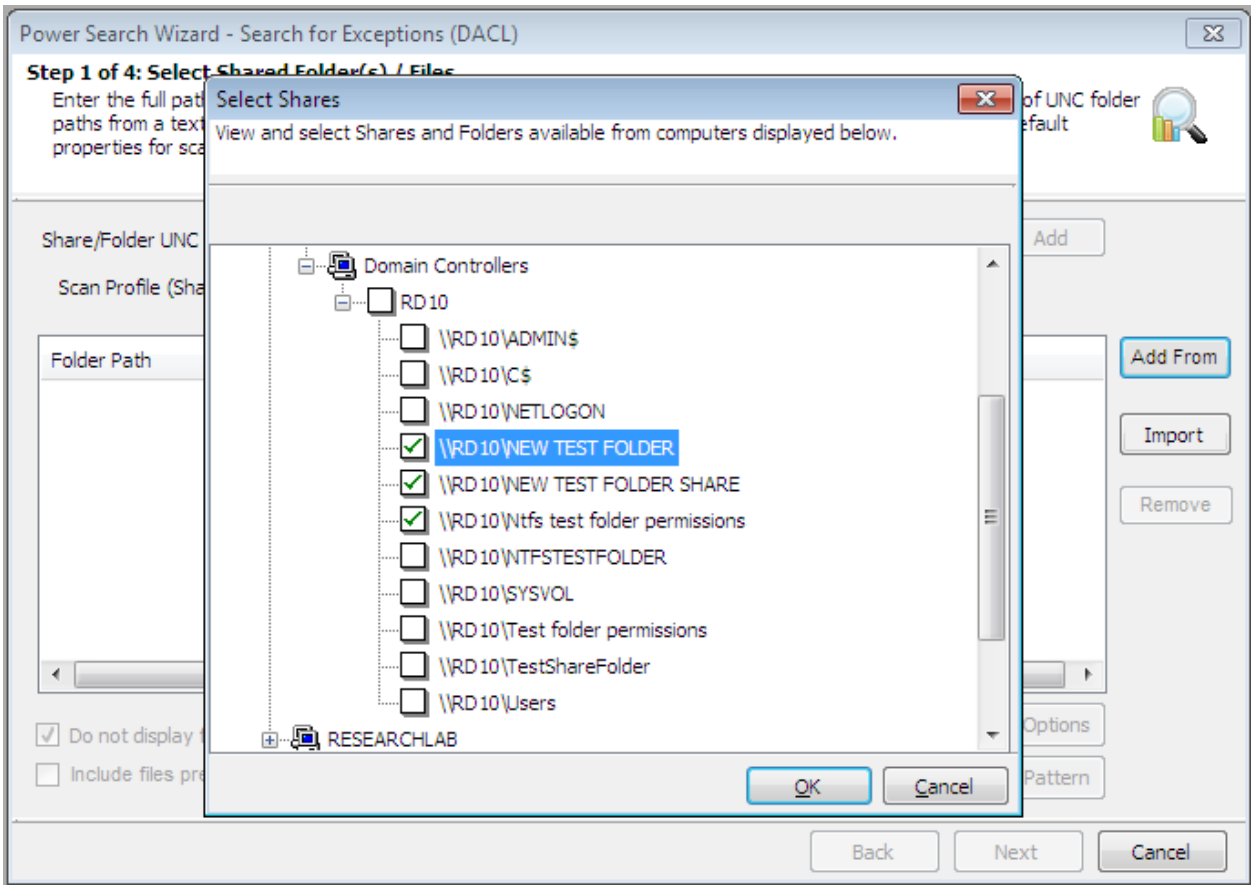
button under Power Search.

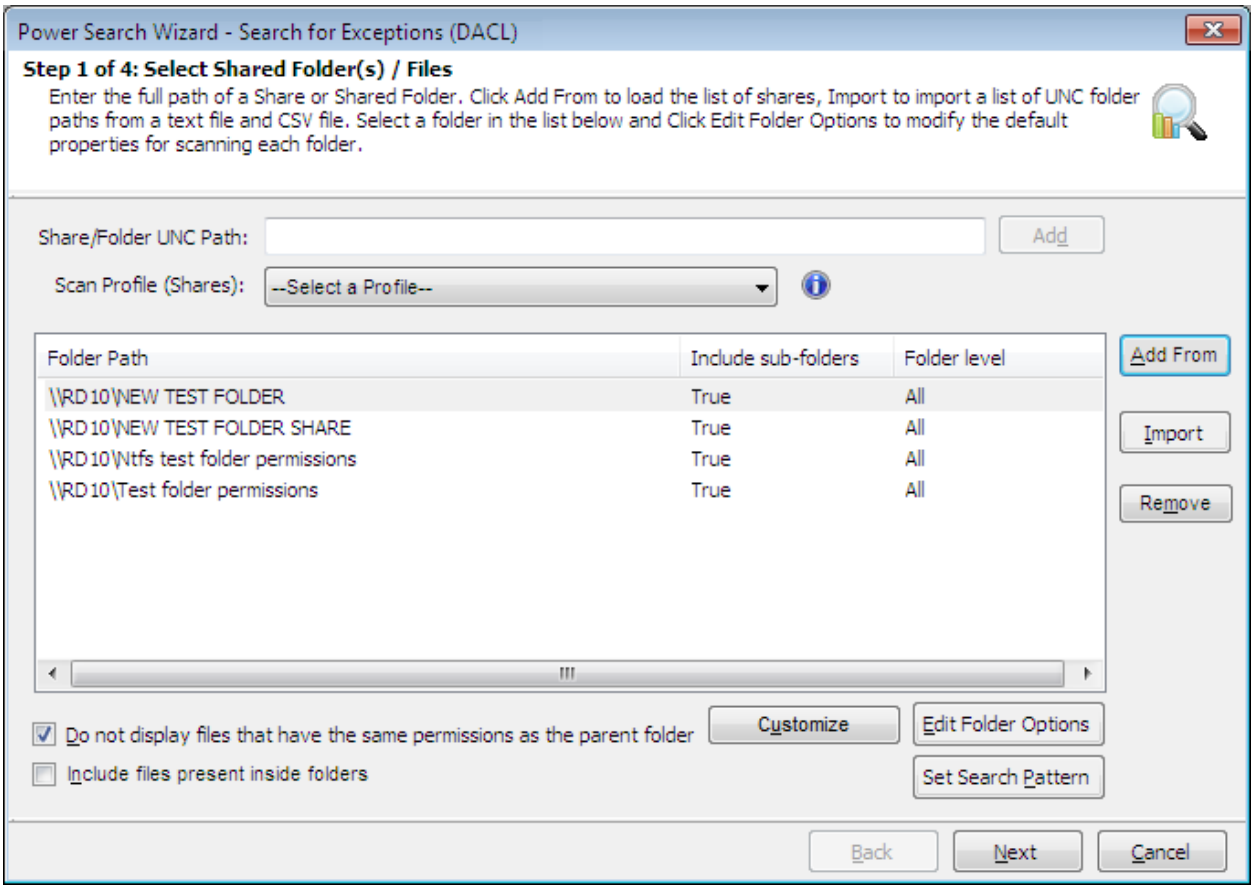
The Power Search window will be displayed as shown below:

Step 1: Select Shared Folder(s)/Files

Select one or more servers to enumerate its Shared Folder(s)/Files.


Power Search Wizard - Search for Exceptions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel


Power Search Wizard - Search for Exceptions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Select Shares
View and select Shares and Folders available from computers displayed below.
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\Ntfs test folder permissions
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\Test folder permissions
\\RD10\TestShareFolder
\\RD10\Users
RESEARCHLAB
OK
Cancel
Share/Folder UNC
Scan Profile
Folder Path
Add
Add From
Import
Remove
Options
Pattern
Back
Next
Cancel

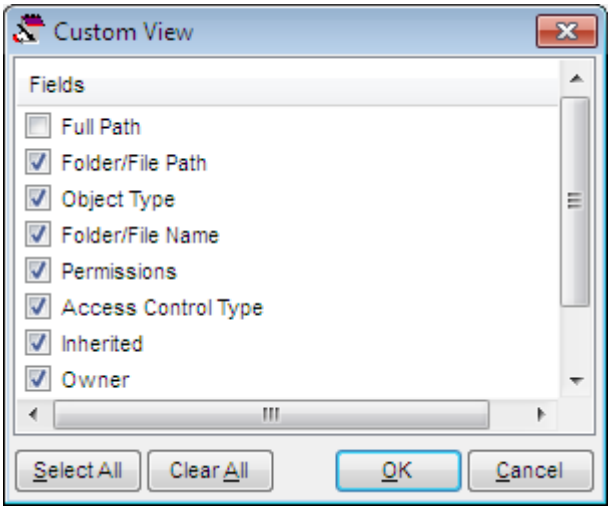

Power Search Wizard - Search for Exceptions (DACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
\\RD10\Test folder permissions
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

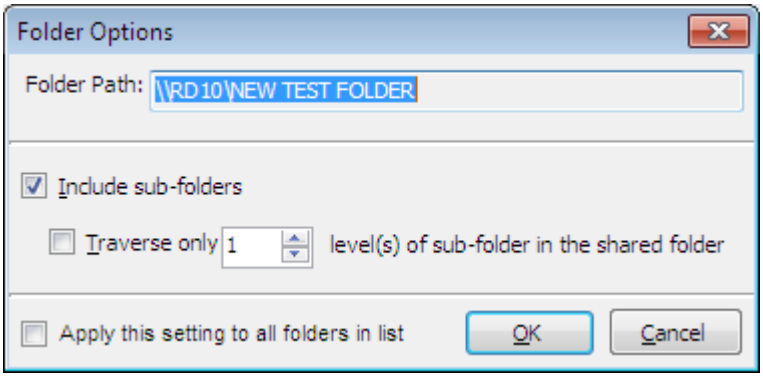
Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select Do not display folders that have same permissions as the parent folder option. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

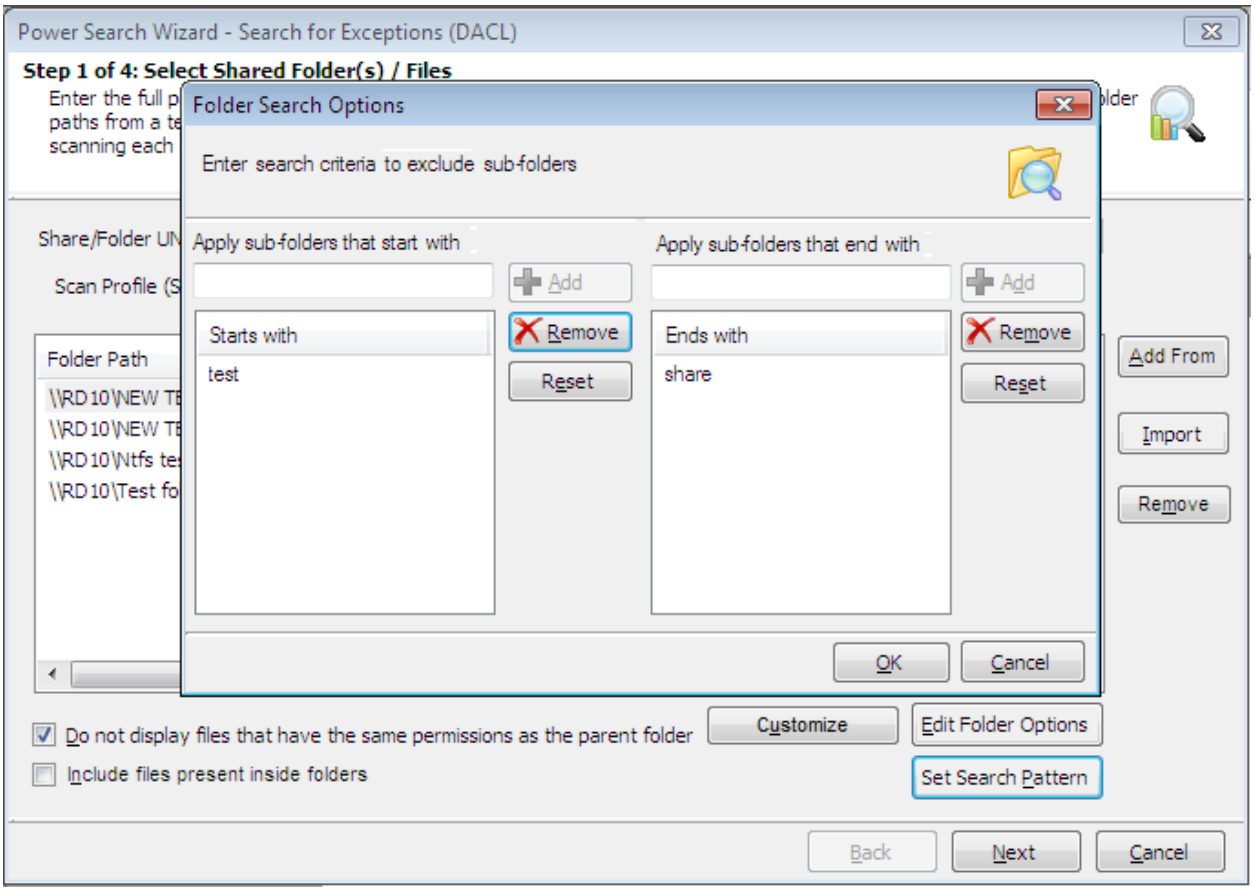
You can use Customize option to exclude some of the fields from the reports, as displayed below:



NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click Edit Folder Options.



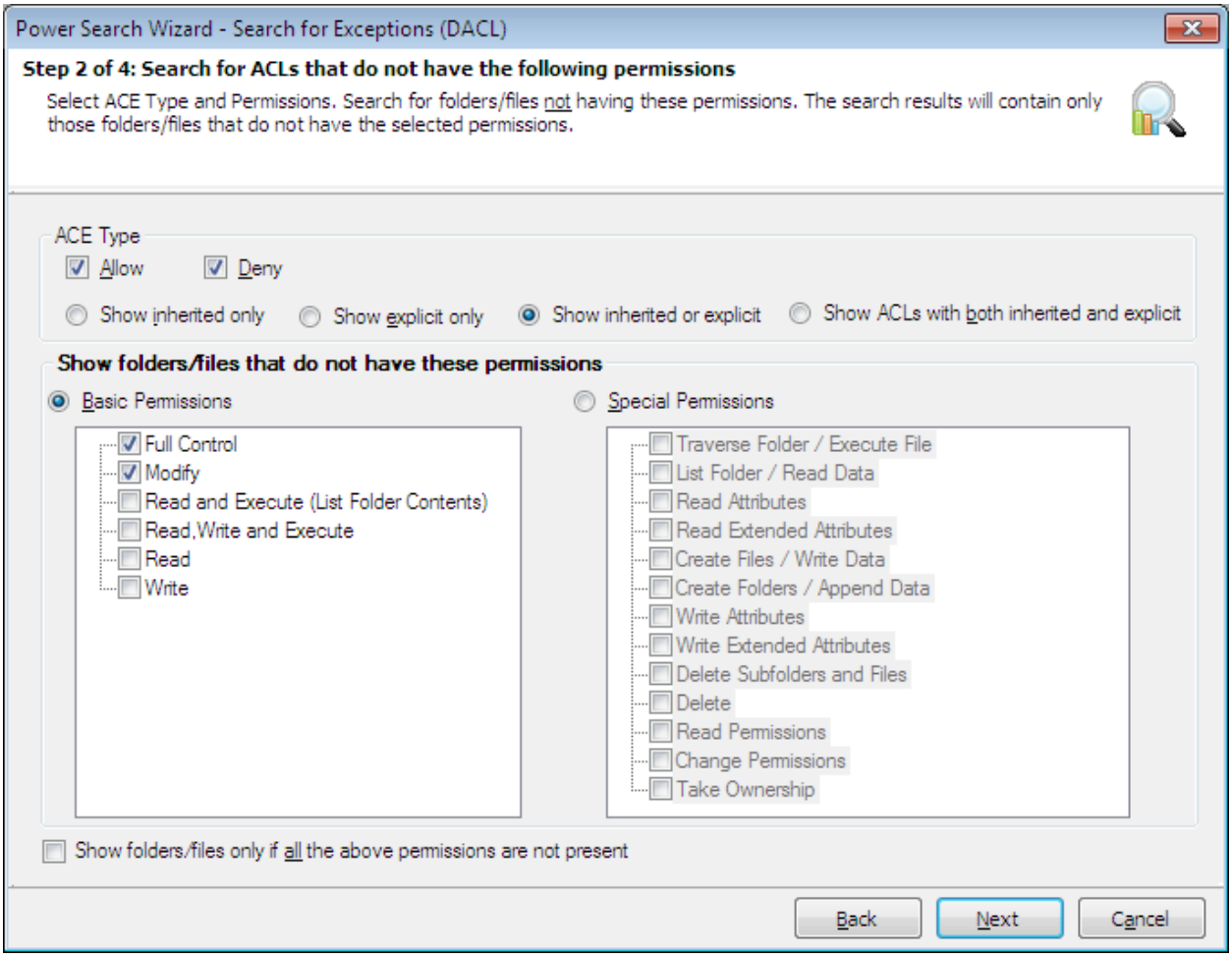
Use Set Search Pattern option to exclude sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example Folder name starts with test, Folder name ends with share.



Click Next to proceed to the next step.

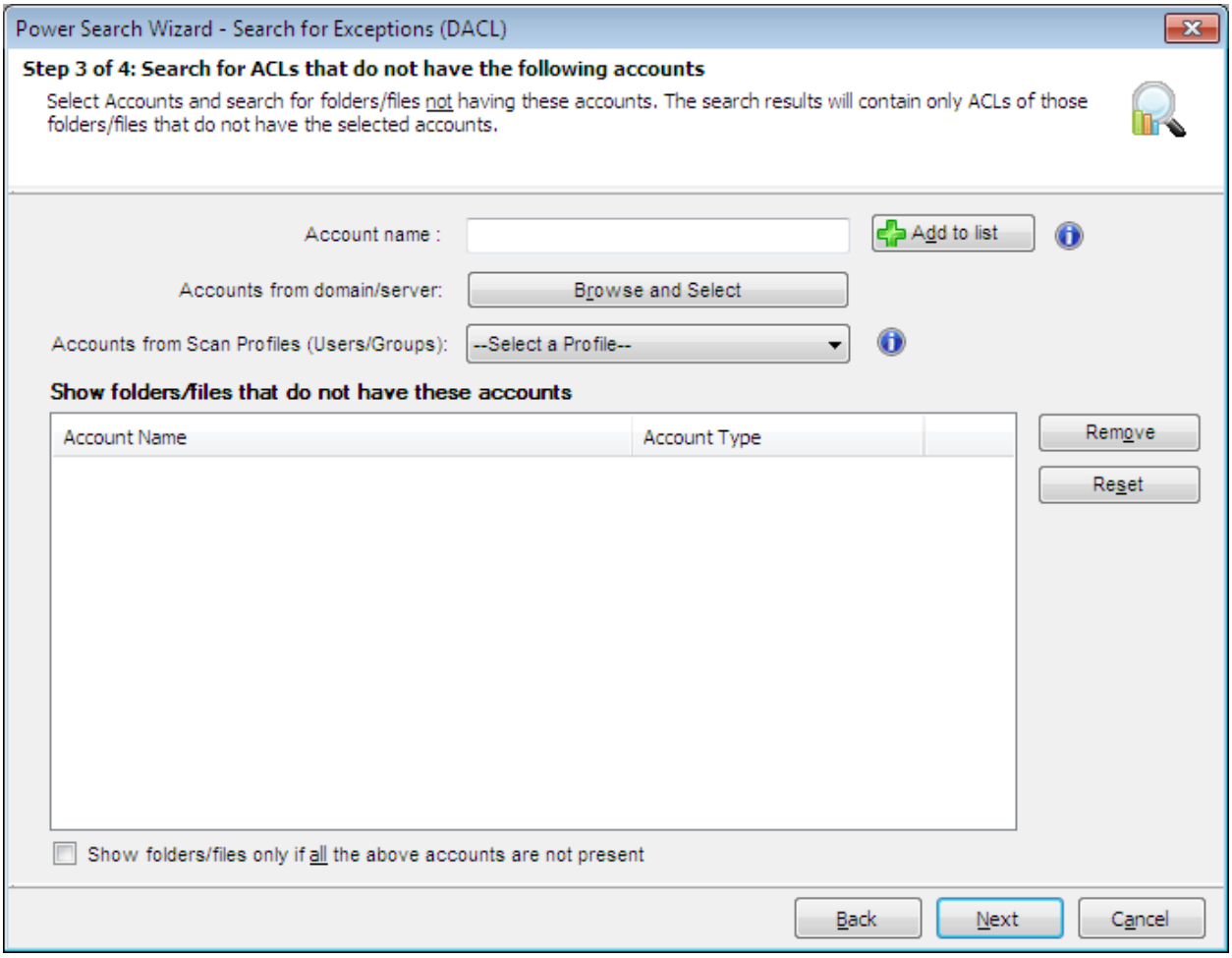
Step 2: Search for ACLs that do not have the following permissions

Select ACE Type and permissions. Search for folders/files that do not have these permissions. The search results will contain only those folders/files that do not have the selected permissions.

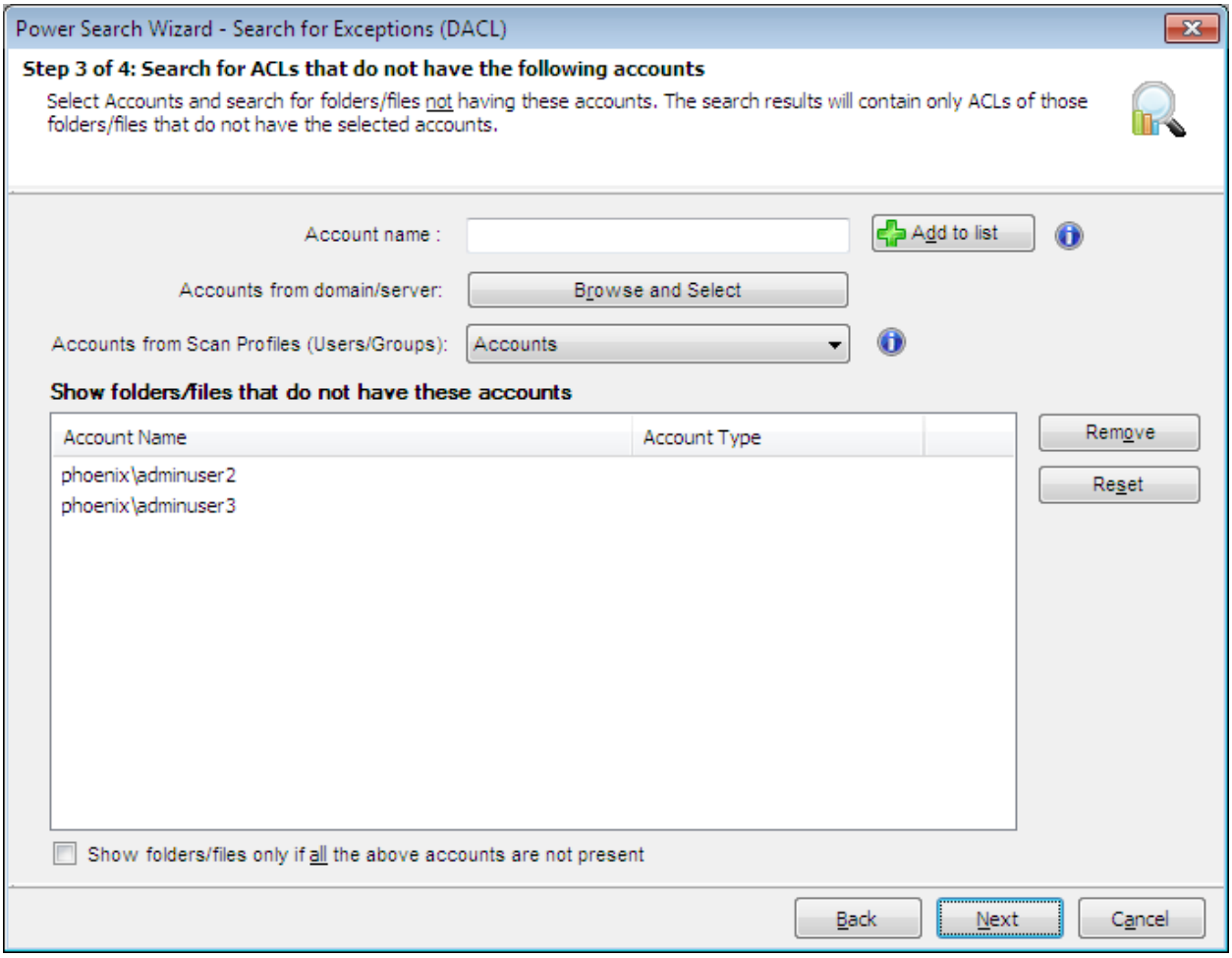

Power Search Wizard - Search for Exceptions (DACL)
Step 2 of 4: Search for ACLs that do not have the following permissions
Select ACE Type and Permissions. Search for folders/files not having these permissions. The search results will contain only those folders/files that do not have the selected permissions.
ACE Type
Allow
Deny
Show inherited only
Show explicit only
Show inherited or explicit
Show ACLs with both inherited and explicit
Show folders/files that do not have these permissions
Basic Permissions
Special Permissions
Full Control
Modify
Read and Execute (List Folder Contents)
Read,Write and Execute
Read
Write
Traverse Folder / Execute File
List Folder / Read Data
Read Attributes
Read Extended Attributes
Create Files / Write Data
Create Folders / Append Data
Write Attributes
Write Extended Attributes
Delete Subfolders and Files
Delete
Read Permissions
Change Permissions
Take Ownership
Show folders/files only if all the above permissions are not present
Back
Next
Cancel

Step 3: Search for ACLs that do not have the following accounts

Select Accounts and search for folders/files that do not have these accounts. The search results will contain only ACLs of those folders/files that do not have the selected accounts.


Power Search Wizard - Search for Exceptions (DACL)
Step 3 of 4: Search for ACLs that do not have the following accounts
Select Accounts and search for folders/files not having these accounts. The search results will contain only ACLs of those folders/files that do not have the selected accounts.
Account name :
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
--Select a Profile--
Show folders/files that do not have these accounts
Account Name
Account Type
Remove
Reset
Show folders/files only if all the above accounts are not present
Back
Next
Cancel

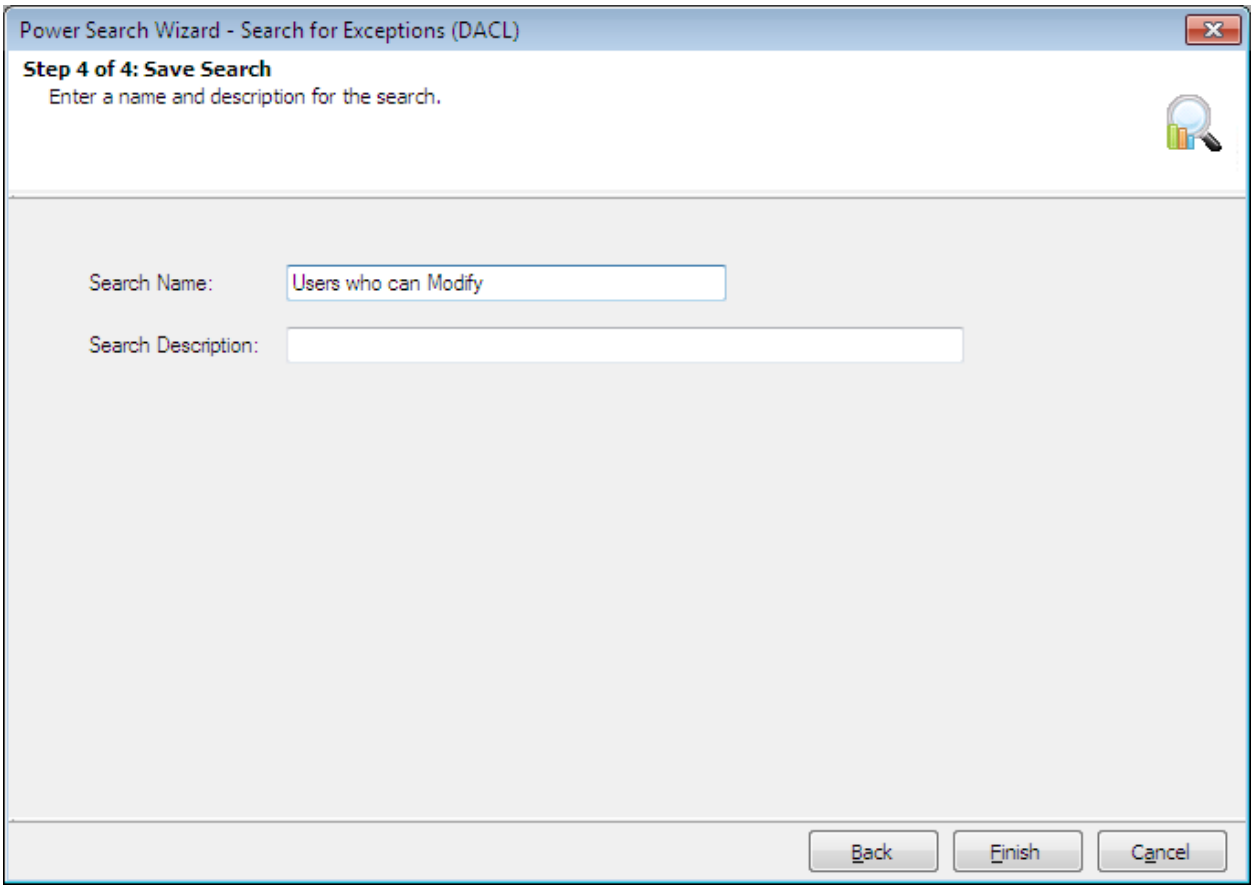
Use Select a Scan Profile (Users/Groups) option to use the users and groups added in the profile as shown below:


Power Search Wizard - Search for Exceptions (DACL)
Step 3 of 4: Search for ACLs that do not have the following accounts
Select Accounts and search for folders/files not having these accounts. The search results will contain only ACLs of those folders/files that do not have the selected accounts.
Account name :
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
Accounts
Show folders/files that do not have these accounts
Account Name
Account Type
phoenix\adminuser2
phoenix\adminuser3
Remove
Reset
Show folders/files only if all the above accounts are not present
Back
Next
Cancel

Click Next to proceed to the Next step.

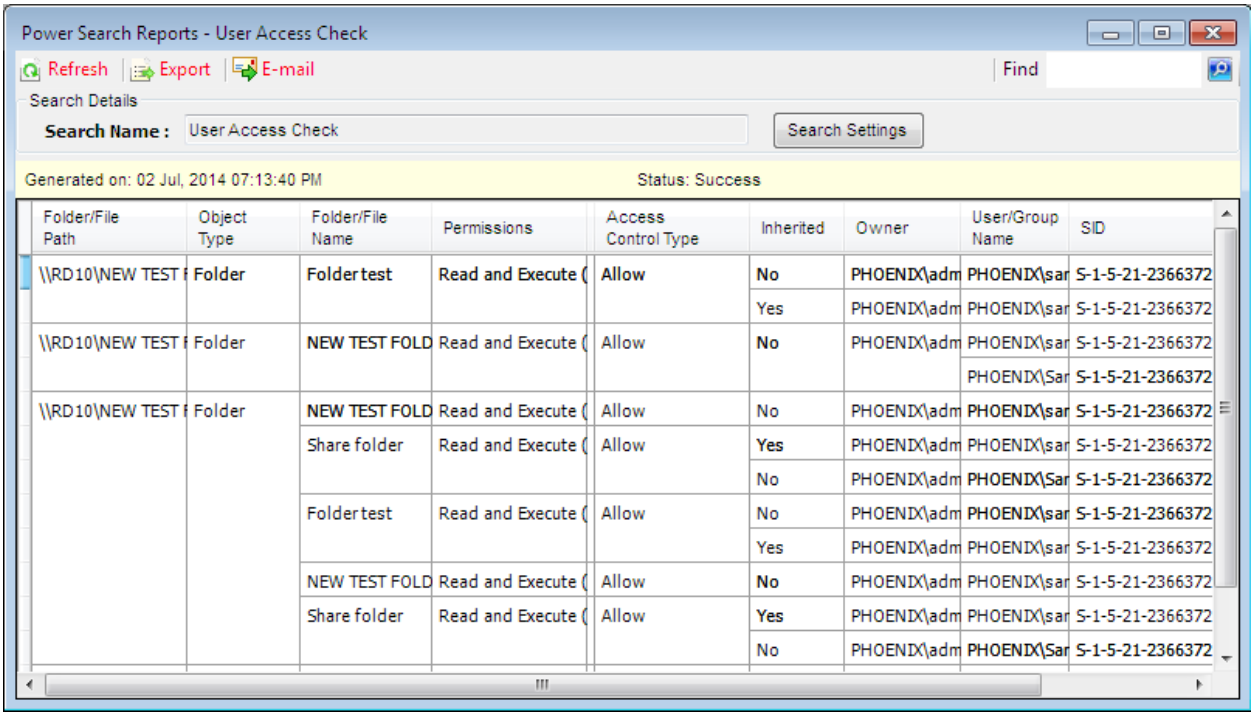
Step 4: Save Search

Enter a name and description for search.

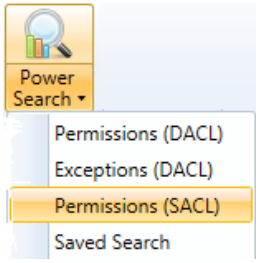


Click Finish to generate the power search report.

After the data collection process is complete, the report would be generated in a report window as shown below:


Power Search Reports - User Access Check
Refresh
Export
E-mail
Find
Search Details
Search Name :
User Access Check
Search Settings
Generated on: 02 Jul, 2014 07:13:40 PM
Status: Success
Folder/File Path
Object Type
Folder/File Name
Permissions
Access Control Type
Inherited
Owner
User/Group Name
SID
\\RD10\NEW TEST
Folder
Folder test
Read and Execute
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
\\RD10\NEW TEST
Folder
NEW TEST FOLD
Read and Execute
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
PHOENIX\Sar
S-1-5-21-2366372
\\RD10\NEW TEST
Folder
NEW TEST FOLD
Read and Execute
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Share folder
Read and Execute
Allow
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
No
PHOENIX\adm
PHOENIX\Sar
S-1-5-21-2366372
Folder test
Read and Execute
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
NEW TEST FOLD
Read and Execute
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Share folder
Read and Execute
Allow
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
No
PHOENIX\adm
PHOENIX\Sar
S-1-5-21-2366372

How to view Power Search Auditing (SACL) Reports?

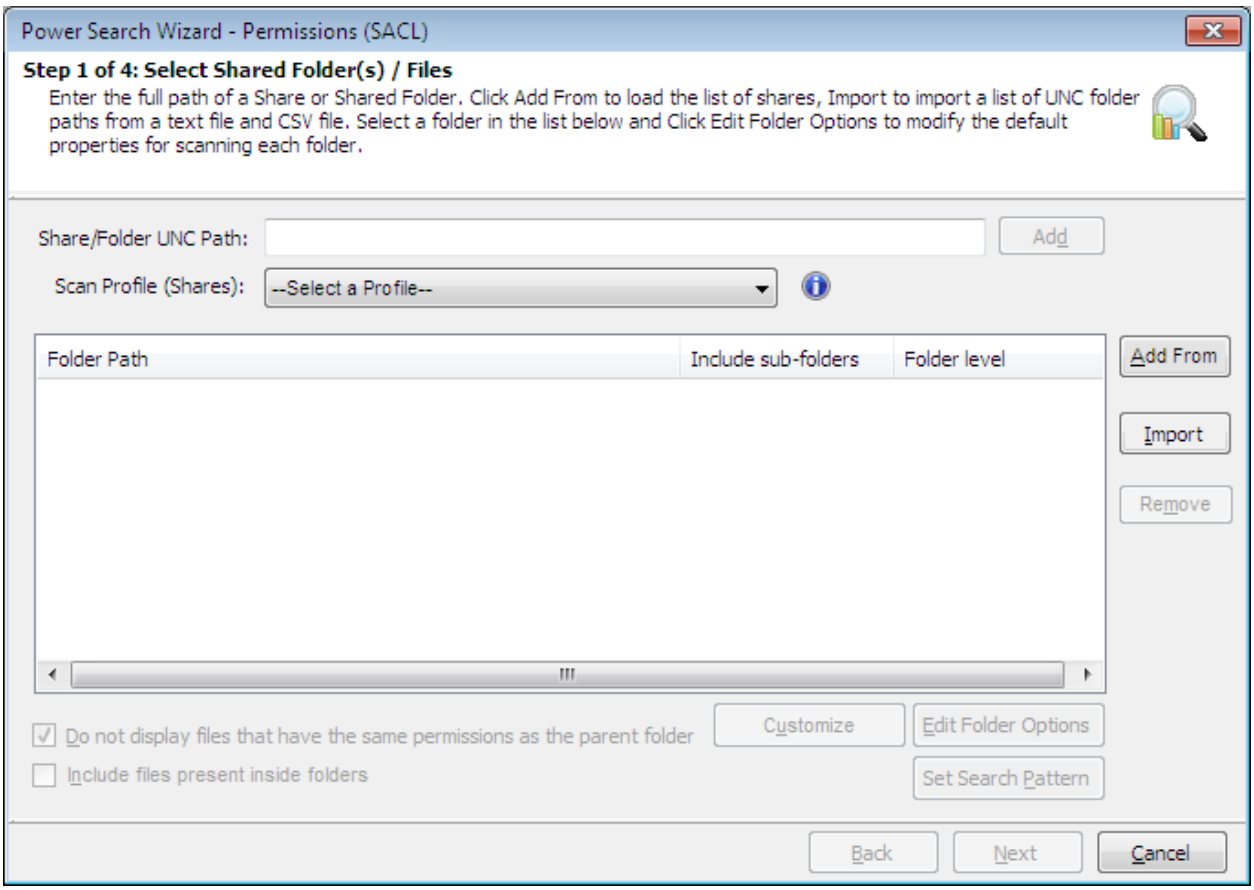


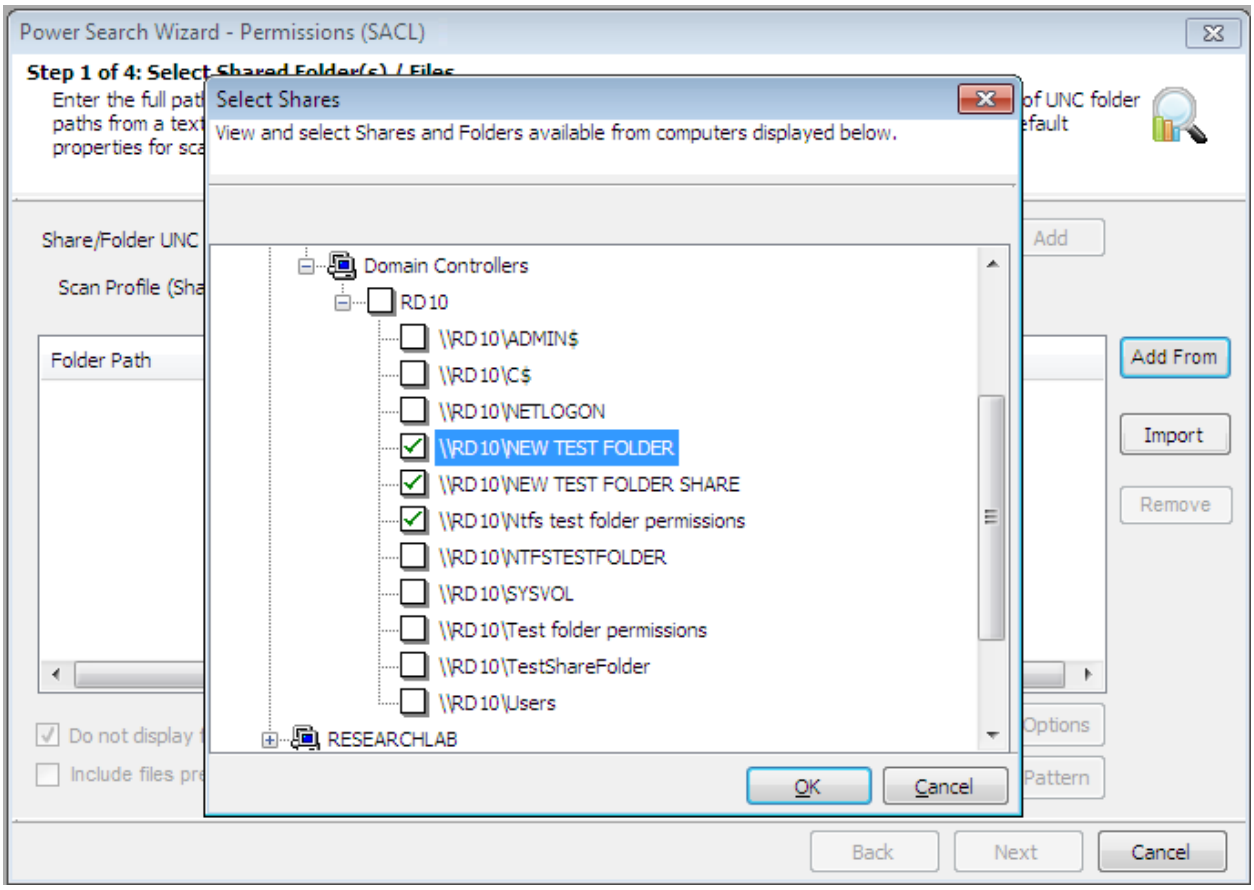
Click on button under Power Search.

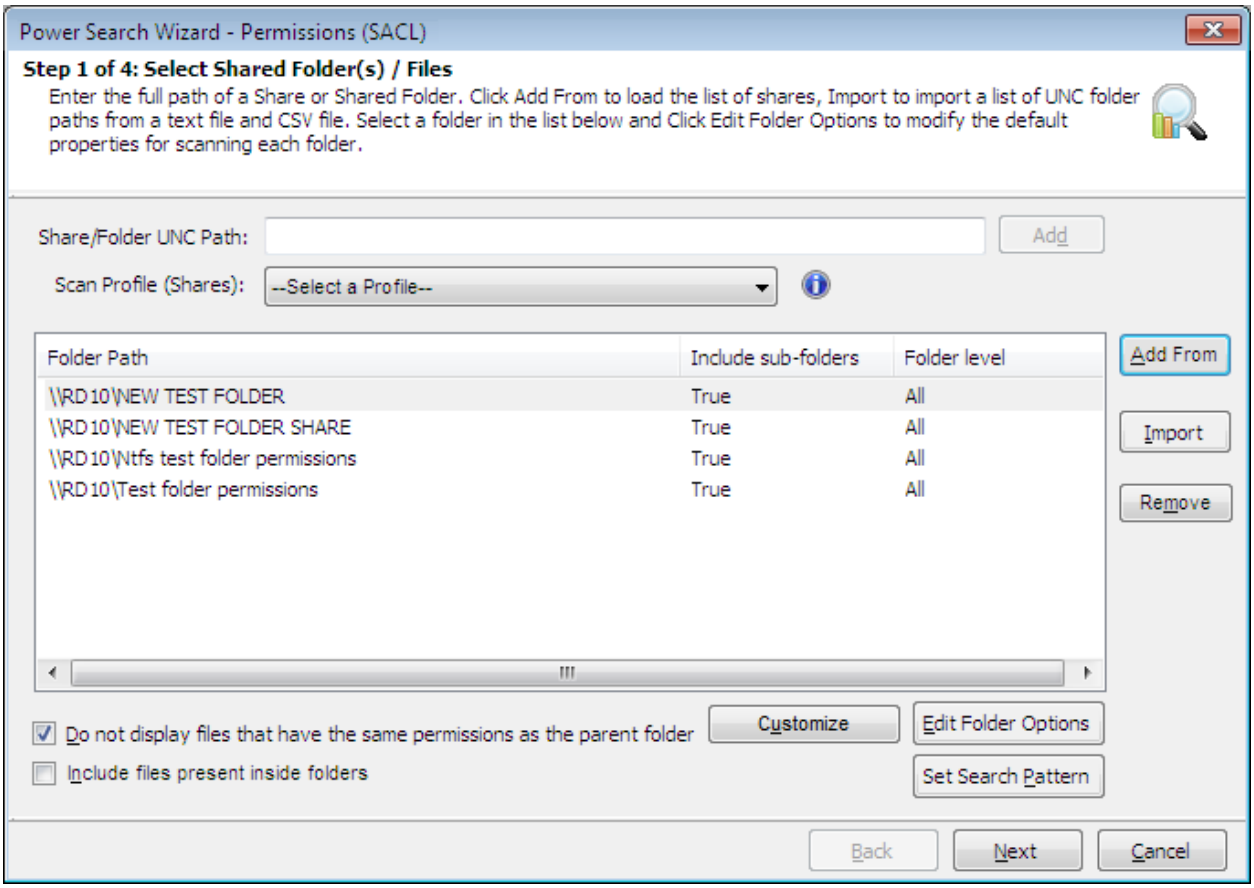
The Power Search window will be displayed as shown below:

Step 1: Select Shared Folder(s)/Files

Select one or more servers to enumerate its Shared Folder(s)/Files


Power Search Wizard - Permissions (SACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel


Power Search Wizard - Permissions (SACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full pat
paths from a text
properties for sca
of UNC folder
efault
Share/Folder UNC
Add
Scan Profile (Sha
Folder Path
Add From
Import
Remove
Do not display f
Include files pre
Options
Pattern
Back
Next
Cancel
Select Shares
View and select Shares and Folders available from computers displayed below.
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\Ntfs test folder permissions
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\Test folder permissions
\\RD10\TestShareFolder
\\RD10\Users
RESEARCHLAB
OK
Cancel

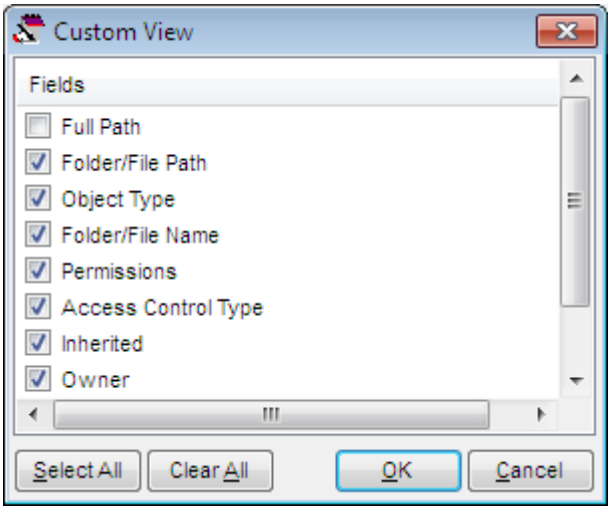

Power Search Wizard - Permissions (SACL)
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
\\RD10\Test folder permissions
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Customize
Edit Folder Options
Set Search Pattern
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

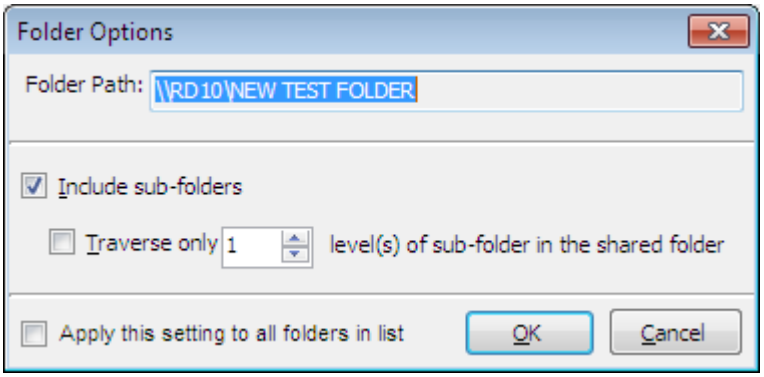
Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

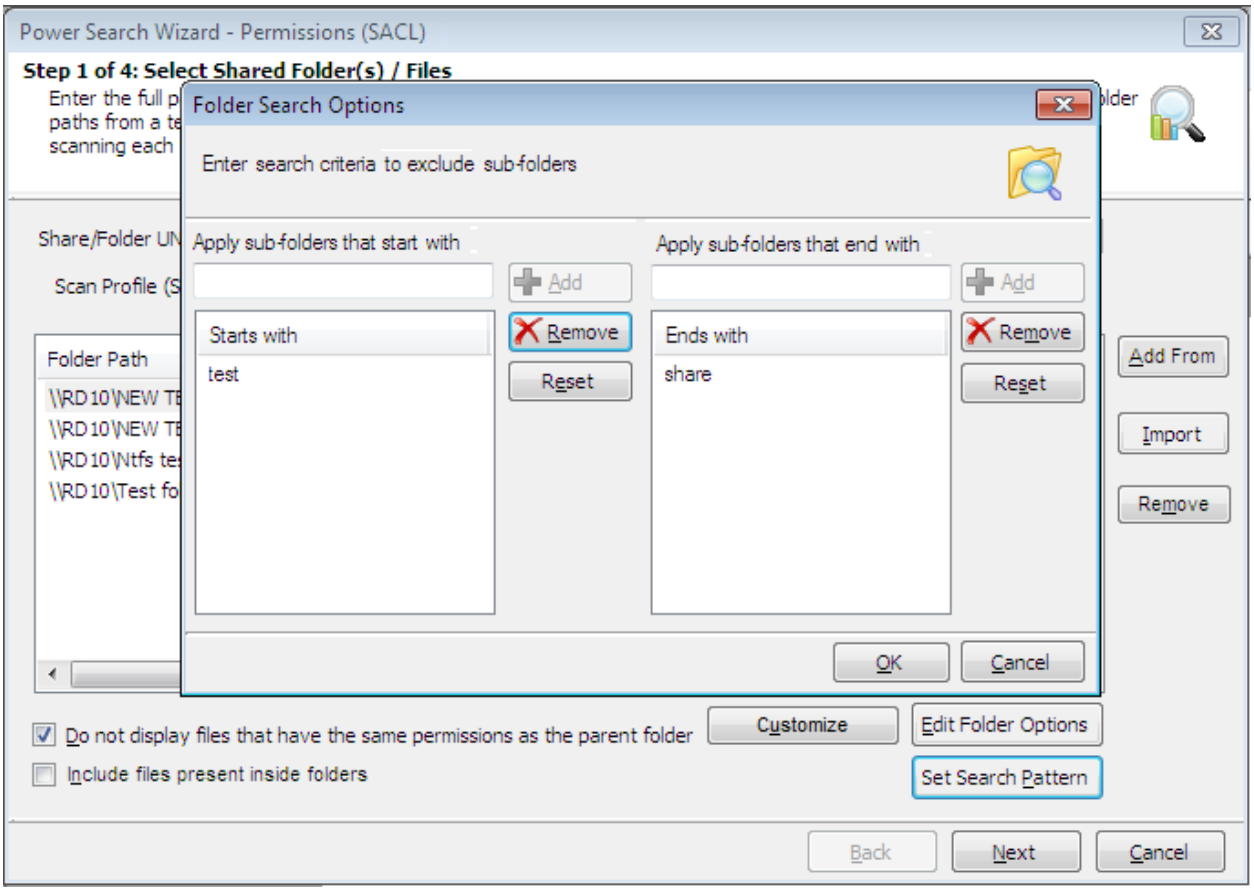
You can use Customize option to exclude some of the fields from the reports, as displayed below:



NTFS Security Auditor defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



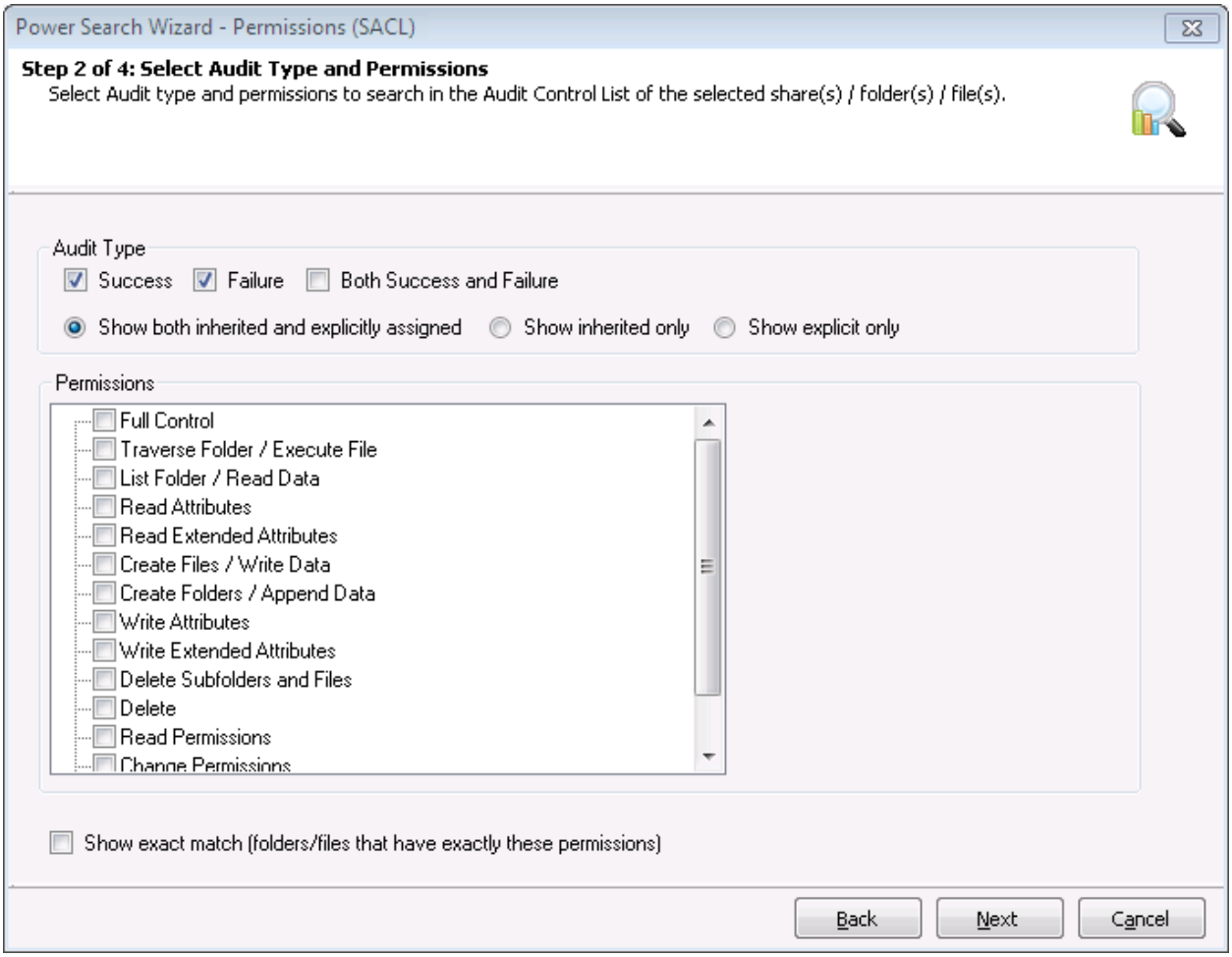
Use **Set Search Pattern** option to exclude sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example Folder name starts with test.



Click **Next** to proceed to the next step.

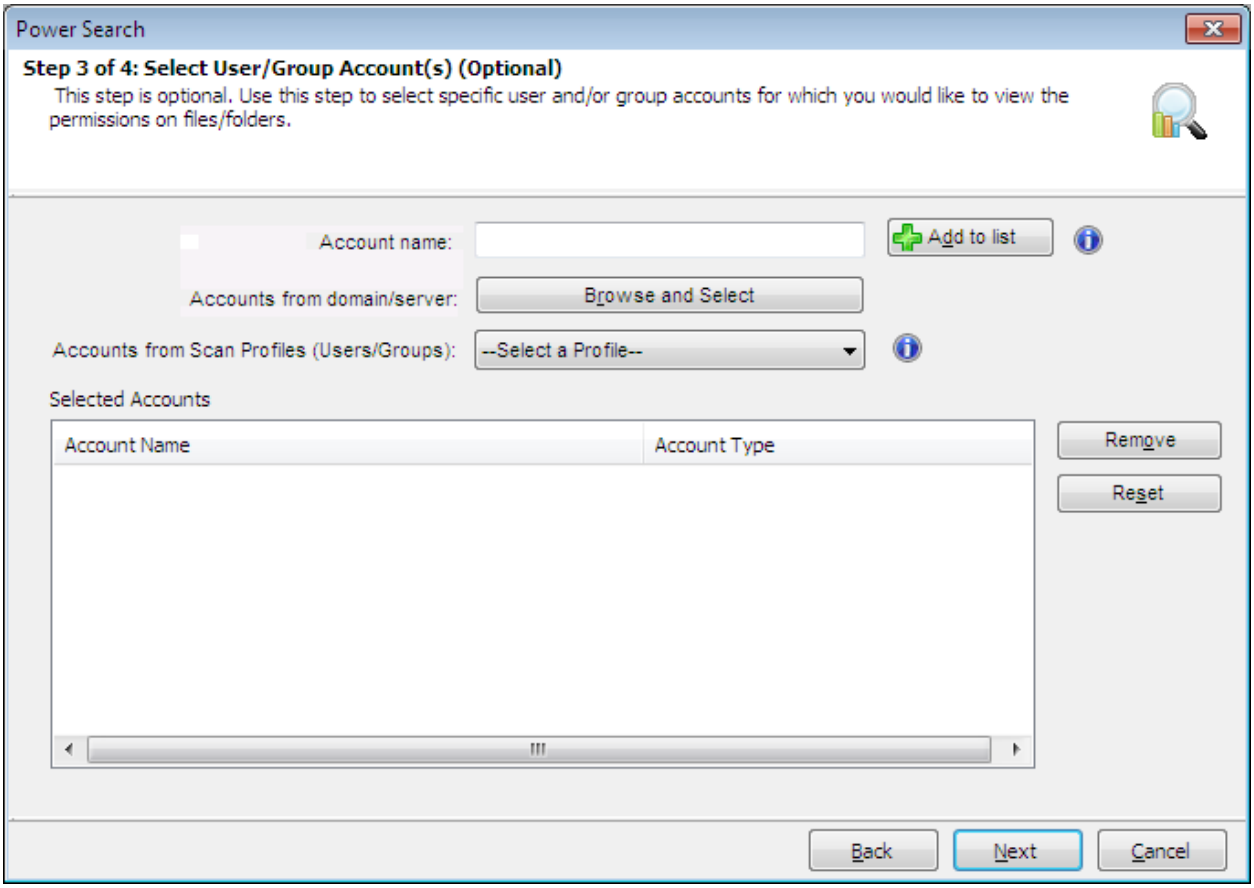
Step 2: Select Audit Type and Permissions

Select Audit Type and permissions to search in the Audit Control List of the selected share(s) / folder(s) /files(s)

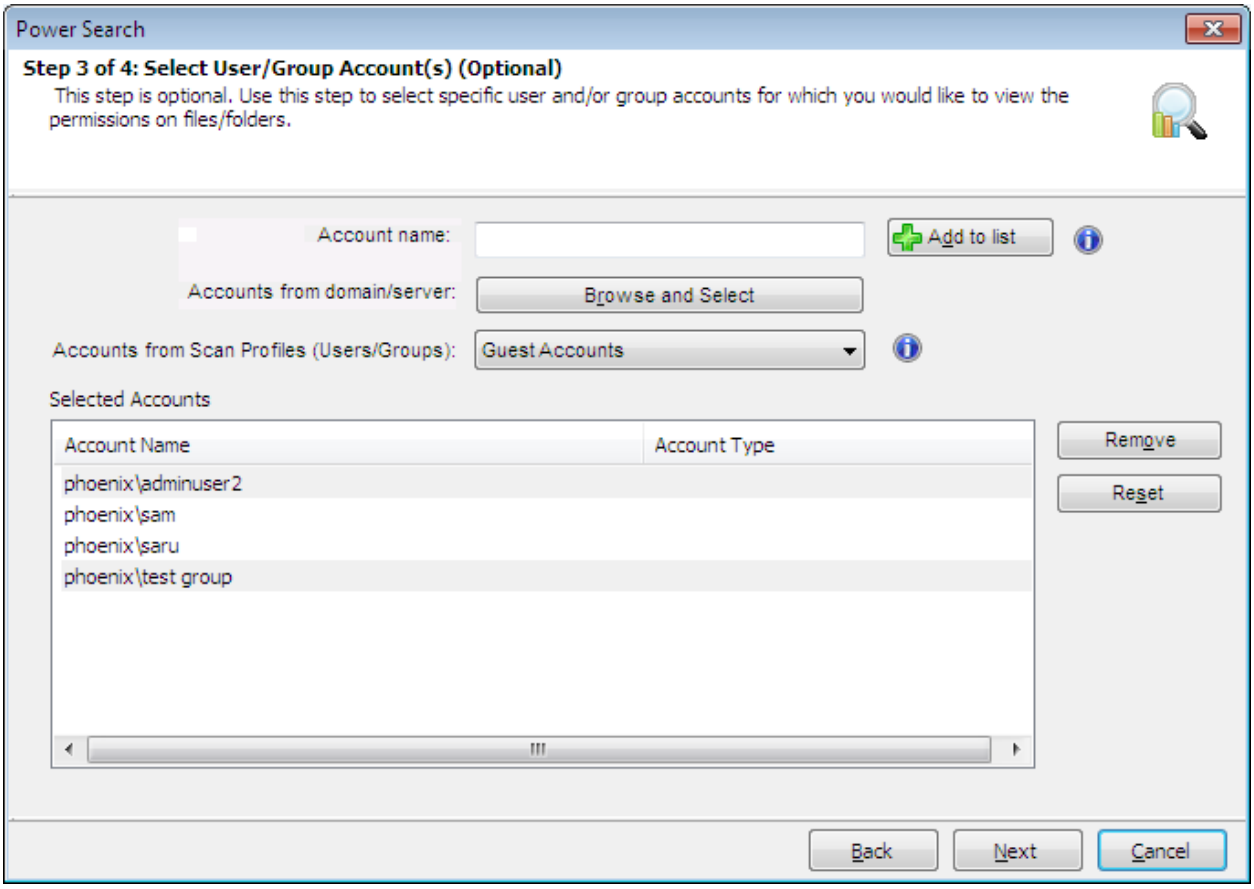


Step 3: User and/or Group Selection

1. Select the user or group, for which you wish to run the search.
2. The selected users will be added to the wizard as shown below:



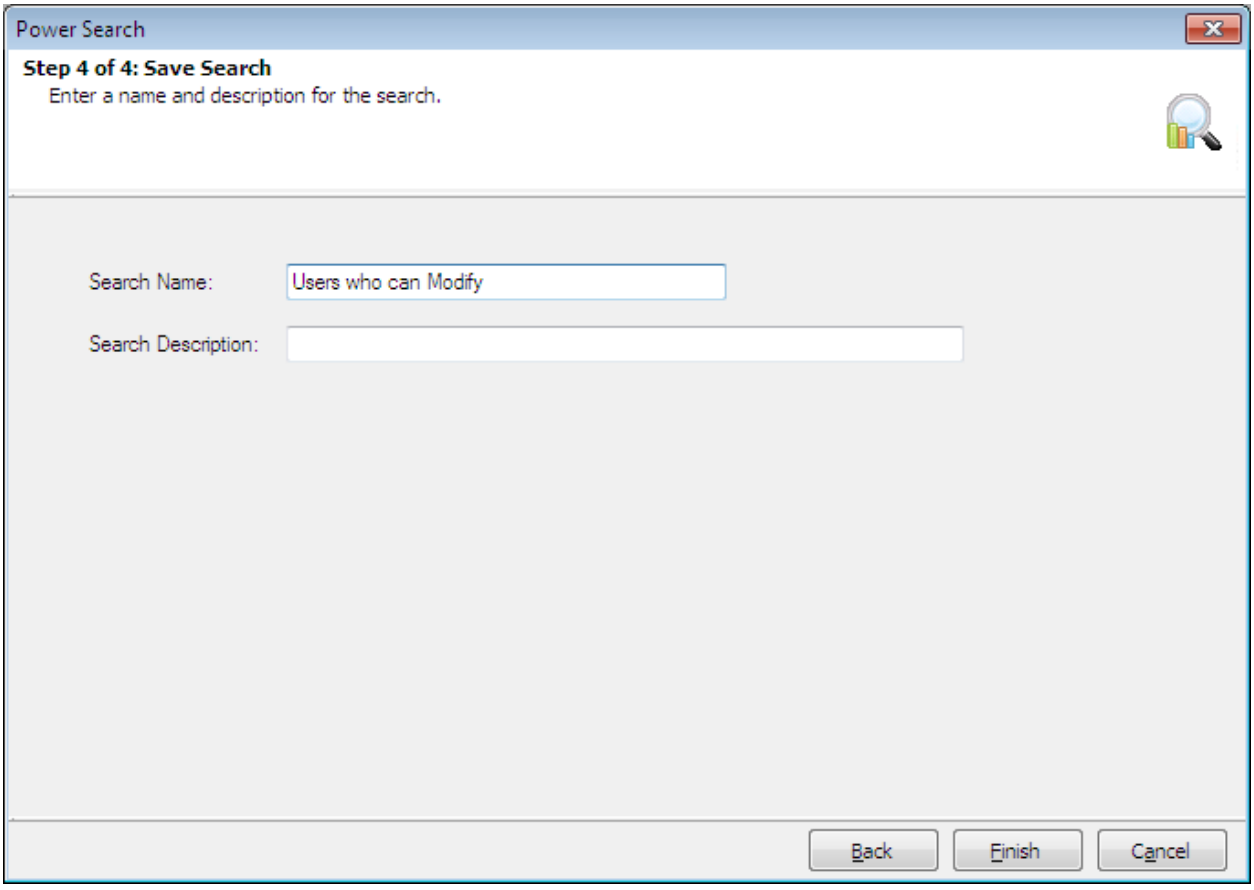
- Use Select a Scan Profile (Users/Groups) option to use the users and groups added in the profile.



- Click **Next** to proceed to the Next step.

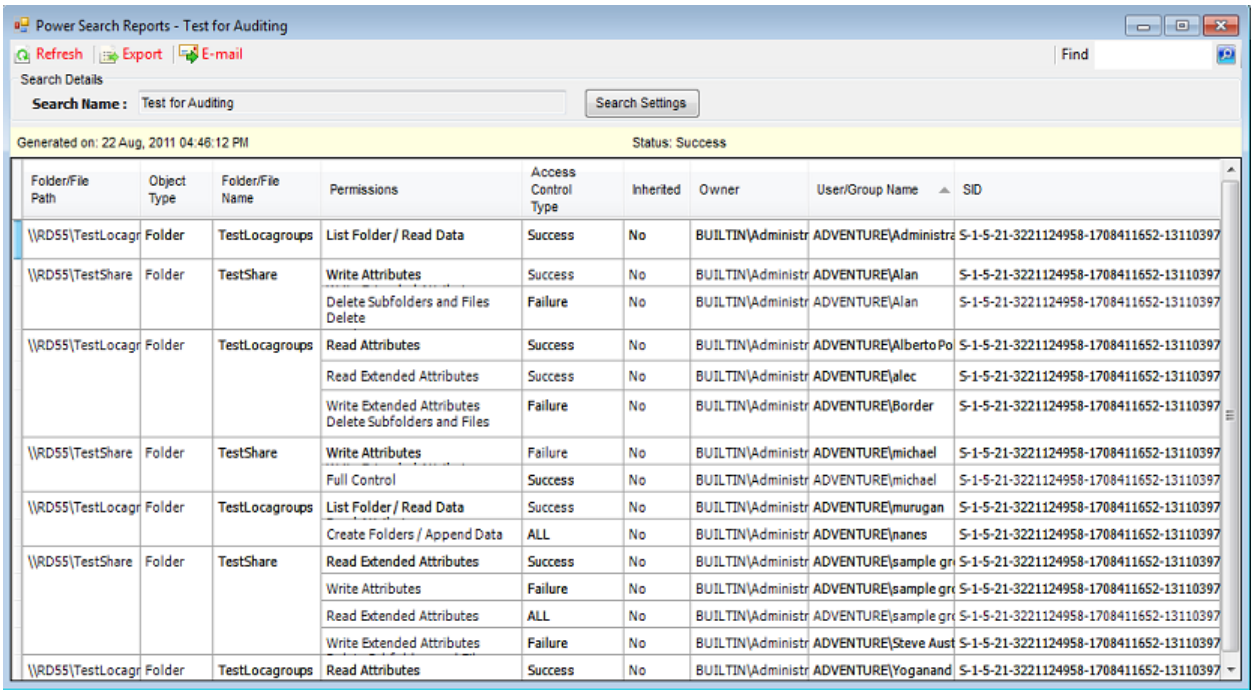
Step 4: Save Search

Enter a name and description for search.



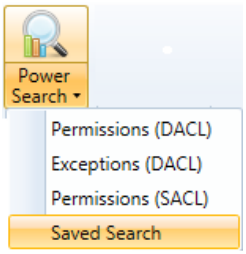
Click **Finish** to generate the power search report.

After the data collection process is complete, the report would be generated in a report window as shown below:

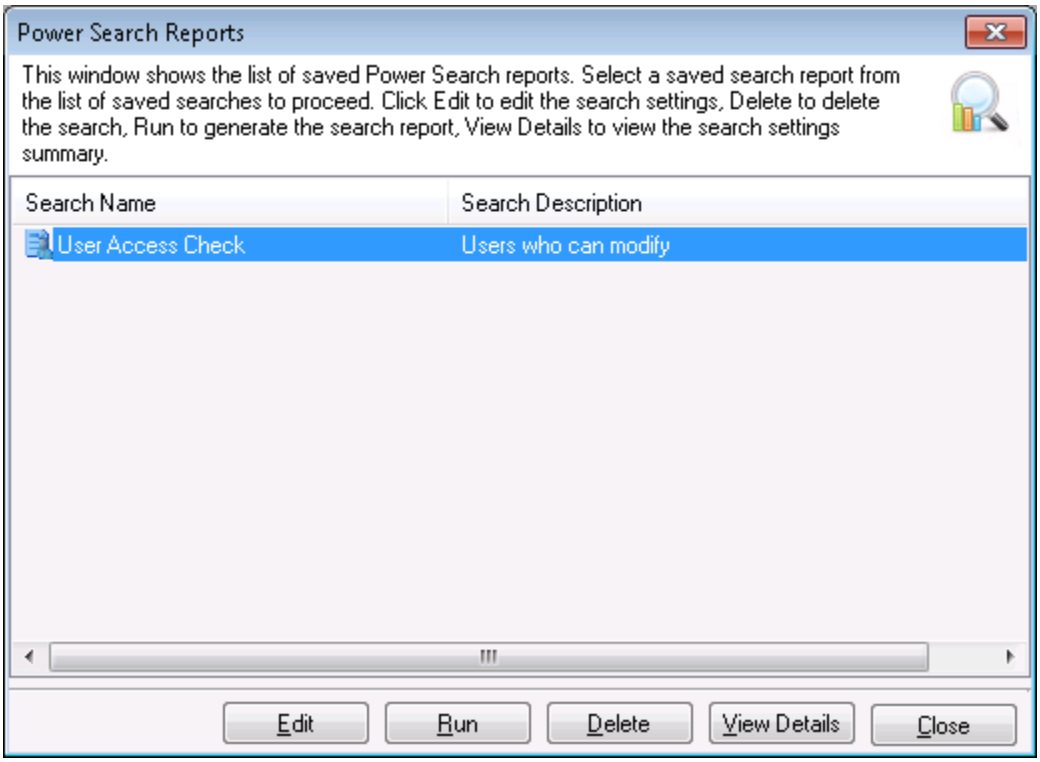


Folder/File Path	Object Type	Folder/File Name	Permissions	Access Control Type	Inherited	Owner	User/Group Name	SID
\\RD55\TestLocagr	Folder	TestLocagroups	List Folder / Read Data	Success	No	BUILTIN\Administr	ADVENTURE\Administra	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestShare	Folder	TestShare	Write Attributes	Success	No	BUILTIN\Administr	ADVENTURE\Alan	S-1-5-21-3221124958-1708411652-13110397
			Delete Subfolders and Files Delete	Failure	No	BUILTIN\Administr	ADVENTURE\Alan	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestLocagr	Folder	TestLocagroups	Read Attributes	Success	No	BUILTIN\Administr	ADVENTURE\Alberto Po	S-1-5-21-3221124958-1708411652-13110397
			Read Extended Attributes	Success	No	BUILTIN\Administr	ADVENTURE\alec	S-1-5-21-3221124958-1708411652-13110397
			Write Extended Attributes Delete Subfolders and Files	Failure	No	BUILTIN\Administr	ADVENTURE\Border	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestShare	Folder	TestShare	Write Attributes	Failure	No	BUILTIN\Administr	ADVENTURE\michael	S-1-5-21-3221124958-1708411652-13110397
			Full Control	Success	No	BUILTIN\Administr	ADVENTURE\michael	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestLocagr	Folder	TestLocagroups	List Folder / Read Data	Success	No	BUILTIN\Administr	ADVENTURE\murugan	S-1-5-21-3221124958-1708411652-13110397
			Create Folders / Append Data	ALL	No	BUILTIN\Administr	ADVENTURE\nanes	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestShare	Folder	TestShare	Read Extended Attributes	Success	No	BUILTIN\Administr	ADVENTURE\sample gr	S-1-5-21-3221124958-1708411652-13110397
			Write Attributes	Failure	No	BUILTIN\Administr	ADVENTURE\sample gr	S-1-5-21-3221124958-1708411652-13110397
			Read Extended Attributes	ALL	No	BUILTIN\Administr	ADVENTURE\sample gr	S-1-5-21-3221124958-1708411652-13110397
			Write Extended Attributes	Failure	No	BUILTIN\Administr	ADVENTURE\Steve Aust	S-1-5-21-3221124958-1708411652-13110397
\\RD55\TestLocagr	Folder	TestLocagroups	Read Attributes	Success	No	BUILTIN\Administr	ADVENTURE\Yoganand	S-1-5-21-3221124958-1708411652-13110397

How to manage Power Search?



Click to launch the saved search(s) window. The windows shows the list of search(s) that were saved over the period of time.


Power Search Reports
This window shows the list of saved Power Search reports. Select a saved search report from the list of saved searches to proceed. Click Edit to edit the search settings, Delete to delete the search, Run to generate the search report, View Details to view the search settings summary.
Search Name
Search Description
User Access Check
Users who can modify
Edit
Run
Delete
View Details
Close

The saved search window allows you to perform the following operations:

- Create a new search
- Run an existing search
- Edit an existing search
- Delete a search
- Preview the settings of a search

Create a new search

1. To create a new search click **New** button in the window. The Power Search Dialog will appear on the screen.
2. Follow the steps as outlined in How to create a power search report?

Run an existing search

1. To **Run** an existing search click Run button in the window. The Power Search report window will appear on the screen and the report will be displayed once the data collection is finished.
2. During edit operation you can modify the search inputs, however, you cannot modify the type of the Scan Profile.

Edit an existing search

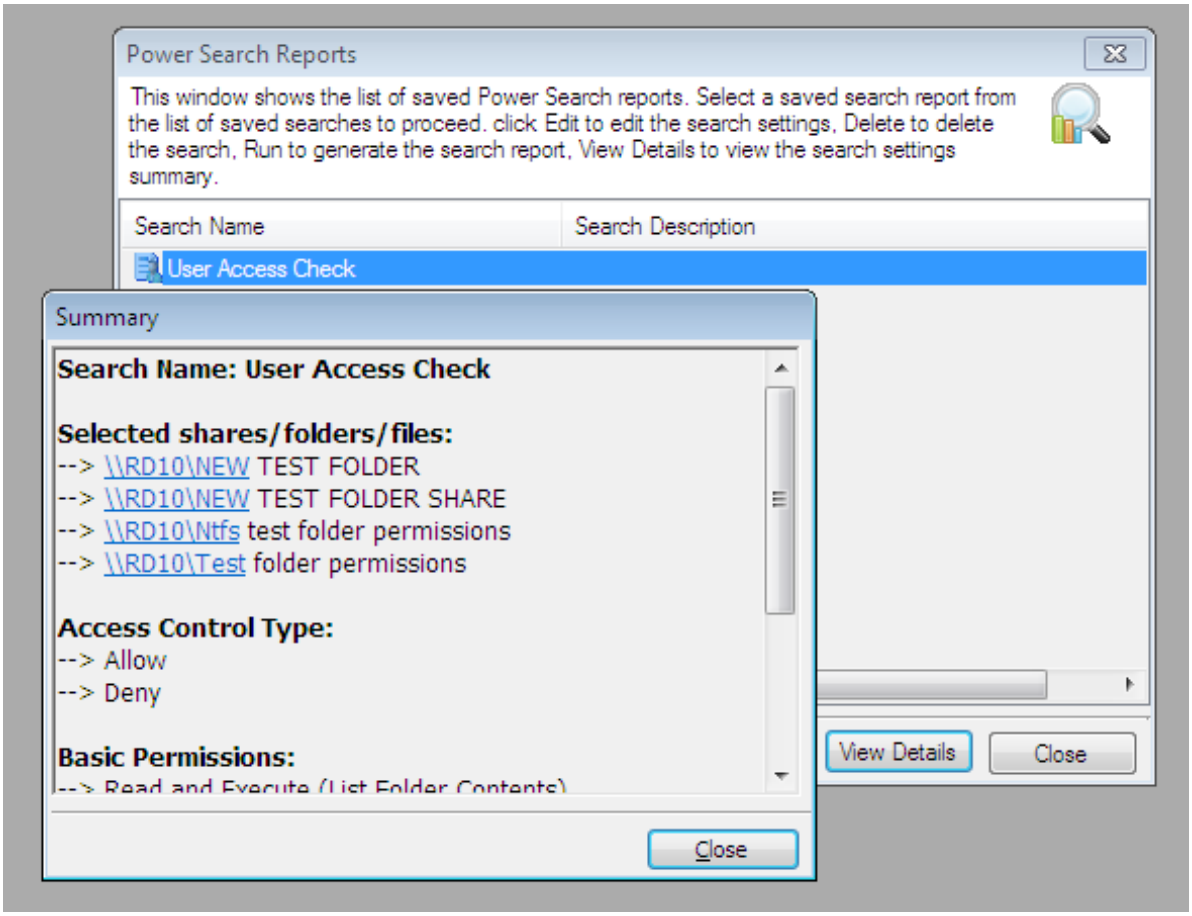
1. To edit an existing search click **Edit** button in the window. The Power Search Dialog will appear on the screen which will allow you to edit the selected search.
2. During edit operation you can modify the computer list, however, you cannot modify the name of the search.

Delete a search

To delete a search, select the search you want to delete, and then click **Delete** button. The selected search will be deleted permanently.

Preview the settings of a search

To preview the settings of a saved search, select a search, and then click **View Details** button. The settings will be displayed in a window as shown below:


Power Search Reports
This window shows the list of saved Power Search reports. Select a saved search report from the list of saved searches to proceed. click Edit to edit the search settings, Delete to delete the search, Run to generate the search report, View Details to view the search settings summary.
Search Name
Search Description
User Access Check
Summary
Search Name: User Access Check
Selected shares/folders/files:
--> \\RD10\NEW TEST FOLDER
--> \\RD10\NEW TEST FOLDER SHARE
--> \\RD10\Ntfs test folder permissions
--> \\RD10\Test folder permissions
Access Control Type:
--> Allow
--> Deny
Basic Permissions:
Close
View Details
Close

Compare ACLs

About Compare ACLs

How to ACLS of Folders?

How to Compare ACLs of a folder with exported ACL data of another folder?

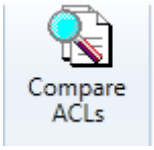
About Compare ACLs

Compare ACLs allows you to compare the inherited and explicit permissions of the shared folders. Select any one of the following options to compare folder ACLs:

Compare ACLs of folders
Compare ACLs of a folder with exported ACL data of another folder

How to Compare ACLs of folders?

This option in Compare ACLs features allows you want to compare all inherited and explicit permissions of two different shared folders. This option will compare only those sub-folders that are available in common (by name) in the specified shared folders.

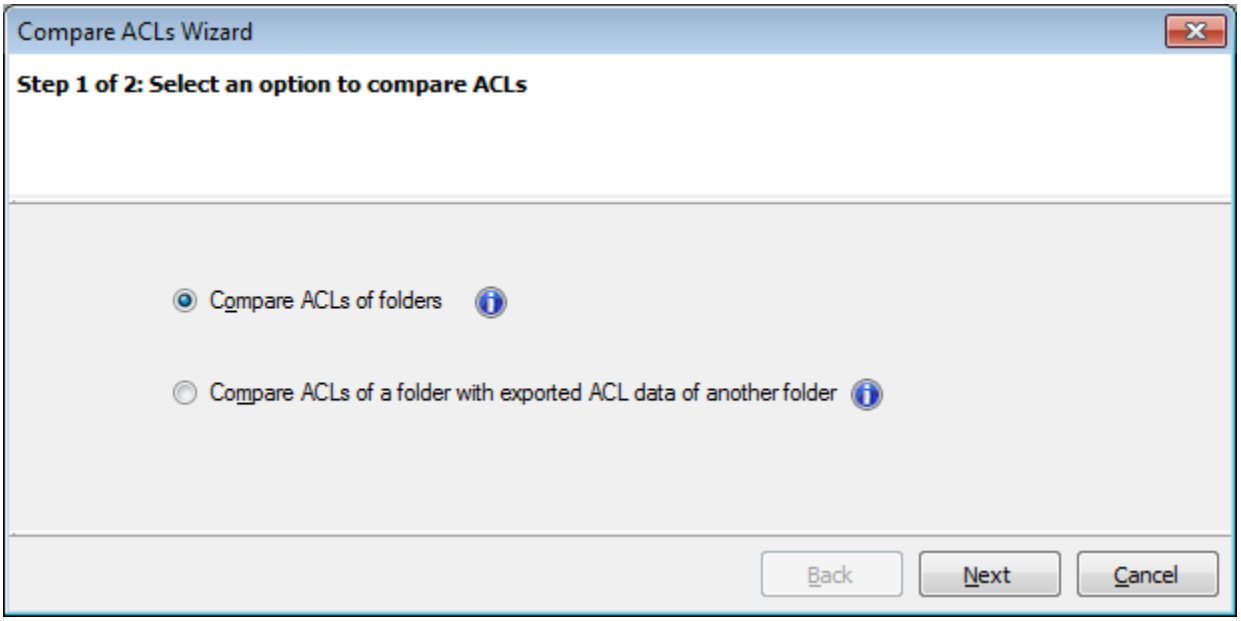
Click on 

button.

The Compare ACLs window will be displayed as shown below:

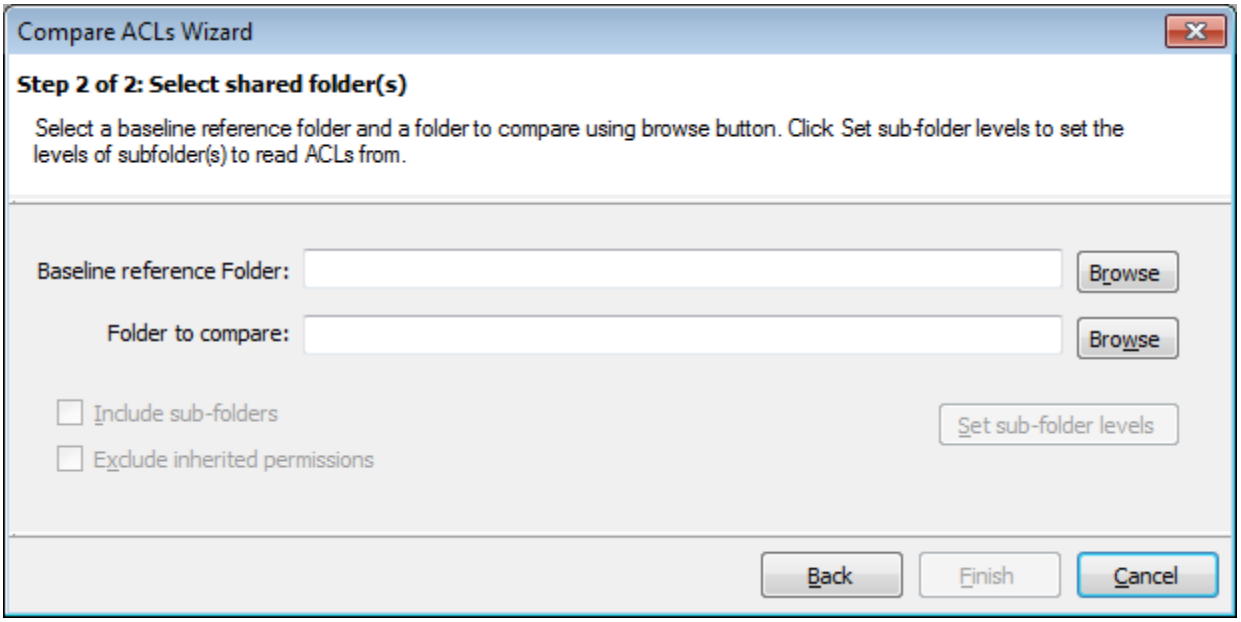
Step 1: Select an option to compare ACLs

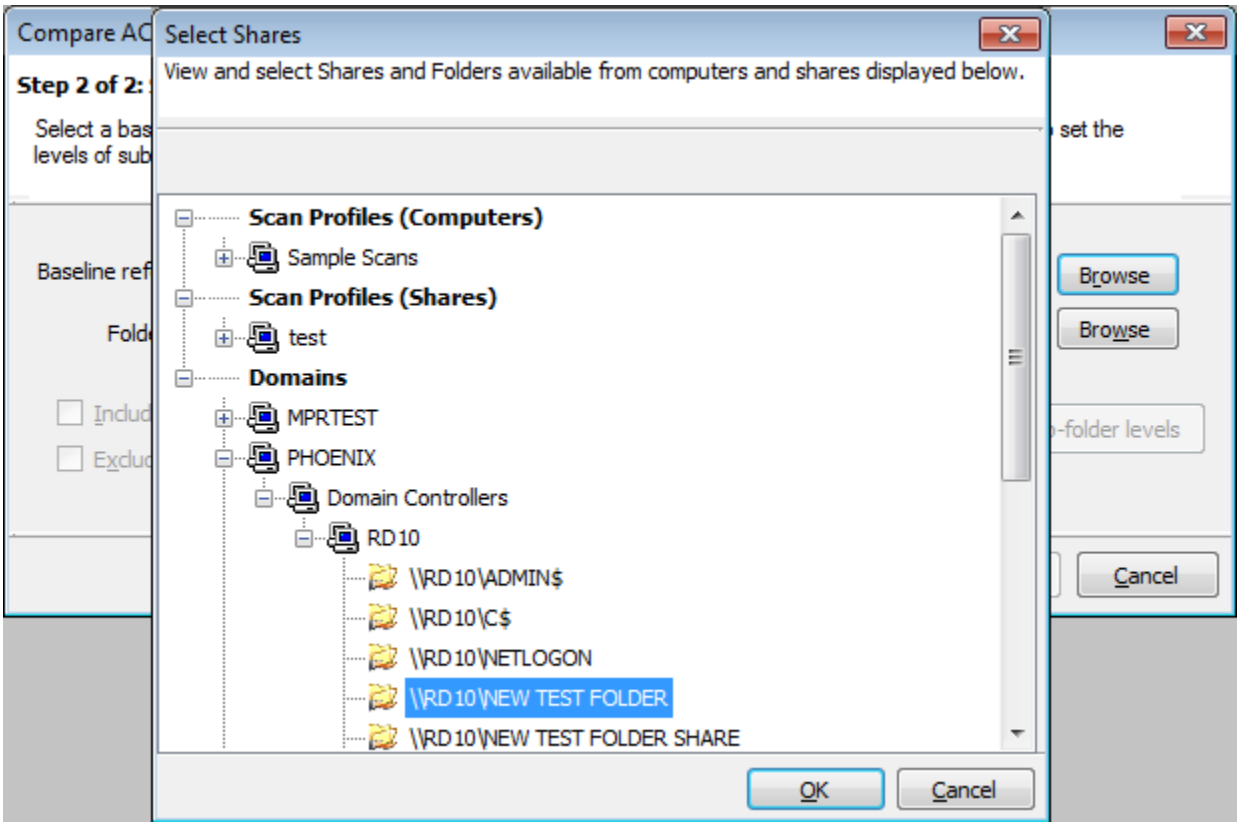
Select Compare ACLs of folders option. Click Next to proceed to the Next step.


Compare ACLs Wizard
Step 1 of 2: Select an option to compare ACLs
Compare ACLs of folders
Compare ACLs of a folder with exported ACL data of another folder
Back
Next
Cancel

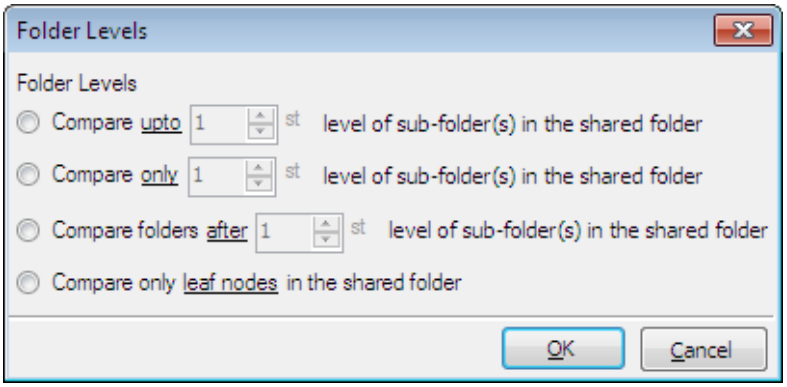
Step 2: Select shared folder(s)

Select a Baseline reference folder and a Folder to compare using the respective browse buttons.


Compare ACLs Wizard
Step 2 of 2: Select shared folder(s)
Select a baseline reference folder and a folder to compare using browse button. Click Set sub-folder levels to set the levels of subfolder(s) to read ACLs from.
Baseline reference Folder:
Browse
Folder to compare:
Browse
Include sub-folders
Exclude inherited permissions
Set sub-folder levels
Back
Finish
Cancel

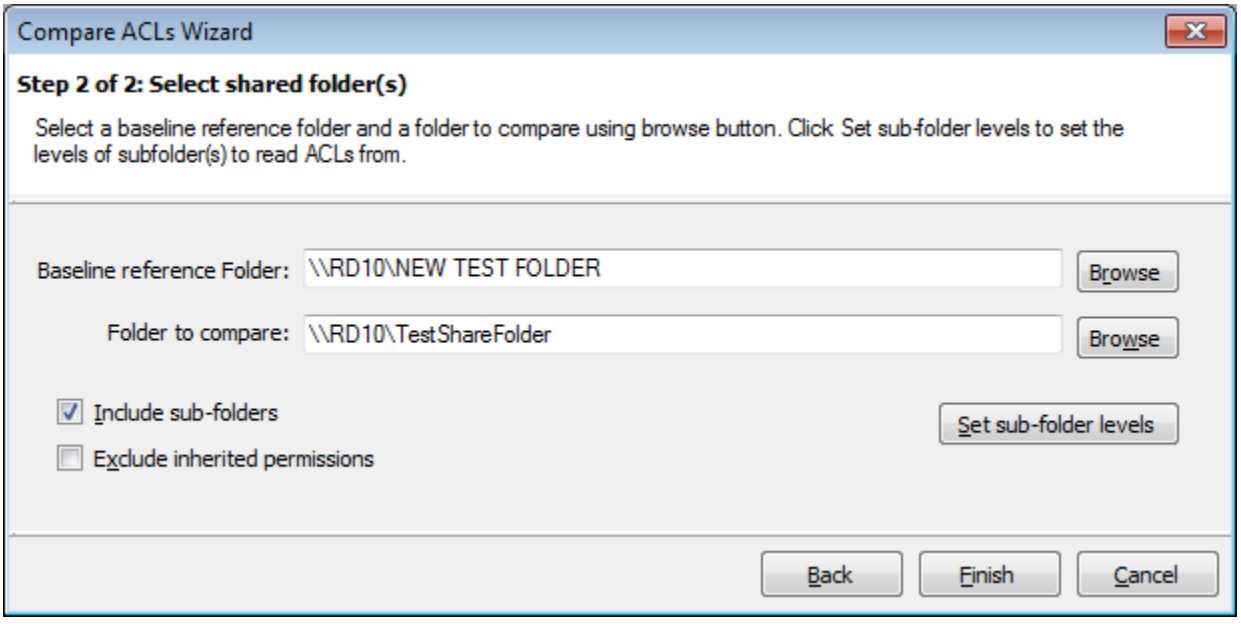


- Include sub-folders: Enabling this option will process the sub-folders of the specified shared folders for comparison.
- Exclude inherited permissions: Enabling this option will exclude inherited permissions of the specified shared folders for comparison.
- Use Set sub-folder levels option to set the levels of subfolder(s) to read ACLs from.

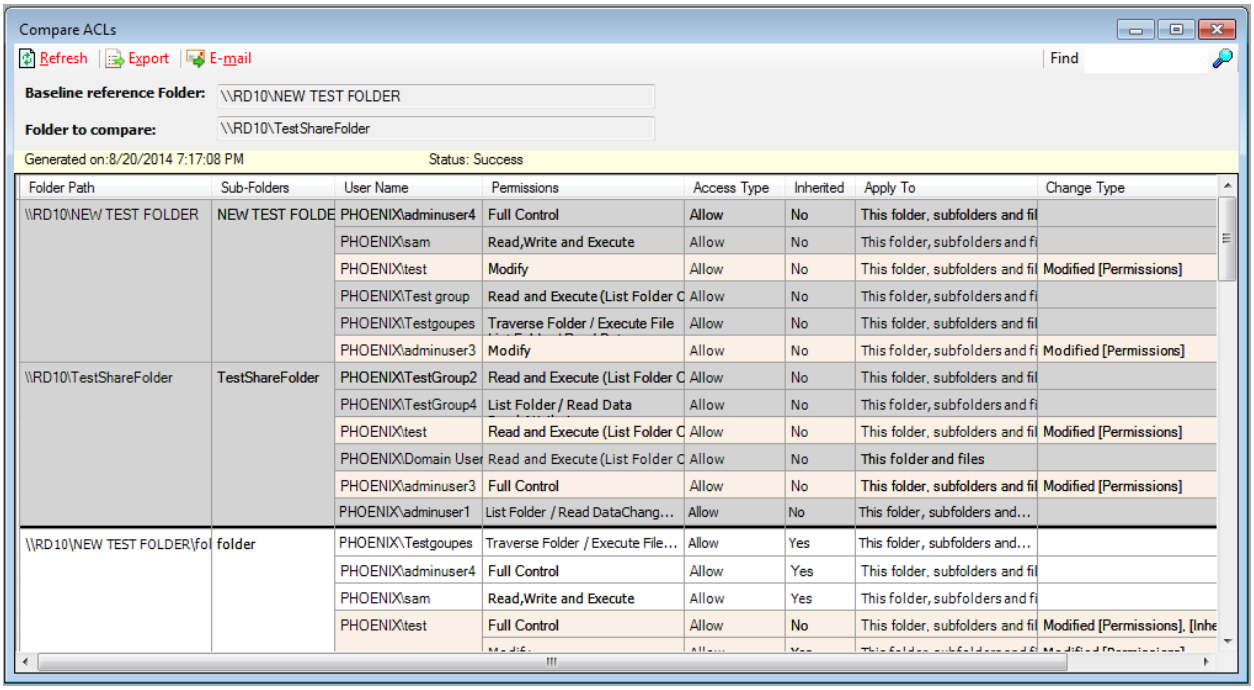

Folder Levels
Folder Levels
Compare upto 1 st level of sub-folder(s) in the shared folder
Compare only 1 st level of sub-folder(s) in the shared folder
Compare folders after 1 st level of sub-folder(s) in the shared folder
Compare only leaf nodes in the shared folder
OK
Cancel

The Sub-folder levels window allows the user to specify the option to enumerate sub-folders for comparing their ACLs, as stated below:

- Compare upto N level(s) of sub-folder(s) in the shared folders: This option will take specified shared folders of sub-folders which are upto the traversal level and compare ACLs only those named sub-folders that are common to the specified shared folders
- Compare only Nth level of sub-folder(s) in the shared folders: This option will take specified shared folders of sub-folders which are in the specified folder level only and compare ACLs only those named sub-folders that are common to the specified shared folders.
- Compare folders after N level(s) of sub-folder(s) in the shared folders: This option will take sub-folders which are after the nth folder level of specified shared folders and compare ACLs only those named sub-folders that are common to the specified shared folders.
- Compare only leaf nodes in the shared folders: This option will take last child (leaf) nodes of specified shared folders and compare ACLs only those named sub-folders that are common to the specified shared folders.

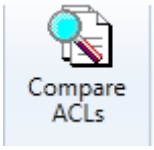

Compare ACLs Wizard
Step 2 of 2: Select shared folder(s)
Select a baseline reference folder and a folder to compare using browse button. Click Set sub-folder levels to set the levels of subfolder(s) to read ACLs from.
Baseline reference Folder: \\RD10\NEW TEST FOLDER
Browse
Folder to compare: \\RD10\TestShareFolder
Browse
Include sub-folders
Exclude inherited permissions
Set sub-folder levels
Back
Finish
Cancel

Click Finish to generate the compared ACLs report.


Compare ACLs
Refresh
Export
E-mail
Find
Baseline reference Folder: \\RD10\NEW TEST FOLDER
Folder to compare: \\RD10\TestShareFolder
Generated on:8/20/2014 7:17:08 PM
Status: Success
Folder Path | Sub-Folders | User Name | Permissions | Access Type | Inherited | Apply To | Change Type
\\RD10\NEW TEST FOLDER | NEW TEST FOLDE | PHOENIX\adminuser4 | Full Control | Allow | No | This folder, subfolders and fil |
PHOENIX\sam | Read,Write and Execute | Allow | No | This folder, subfolders and fi |
PHOENIX\test | Modify | Allow | No | This folder, subfolders and fil | Modified [Permissions]
PHOENIX\Test group | Read and Execute (List Folder C | Allow | No | This folder, subfolders and fi |
PHOENIX\Testgoupes | Traverse Folder / Execute File | Allow | No | This folder, subfolders and fil |
PHOENIX\adminuser3 | Modify | Allow | No | This folder, subfolders and fi | Modified [Permissions]
\\RD10\TestShareFolder | TestShareFolder | PHOENIX\TestGroup2 | Read and Execute (List Folder C | Allow | No | This folder, subfolders and fil |
PHOENIX\TestGroup4 | List Folder / Read Data | Allow | No | This folder, subfolders and fi |
PHOENIX\test | Read and Execute (List Folder C | Allow | No | This folder, subfolders and fil | Modified [Permissions]
PHOENIX\Domain User | Read and Execute (List Folder C | Allow | No | This folder and files |
PHOENIX\adminuser3 | Full Control | Allow | No | This folder, subfolders and fil | Modified [Permissions]
PHOENIX\adminuser1 | List Folder / Read DataChang... | Allow | No | This folder, subfolders and... |
\\RD10\NEW TEST FOLDER\fol | folder | PHOENIX\Testgoupes | Traverse Folder / Execute File... | Allow | Yes | This folder, subfolders and... |
PHOENIX\adminuser4 | Full Control | Allow | Yes | This folder, subfolders and fil |
PHOENIX\sam | Read,Write and Execute | Allow | Yes | This folder, subfolders and fi |
PHOENIX\test | Full Control | Allow | No | This folder, subfolders and fil | Modified [Permissions], [Inhe

How to Compare ACLs of a folder with exported ACL data of another folder?

This option in Compare ACLs features allows you to find out the differences between a past snapshot of ACLs and the current ACLs of a shared folder. This option will compare only those sub-folders that are available in common (by name) in the specified shared folder and the shared folder in the exported report.

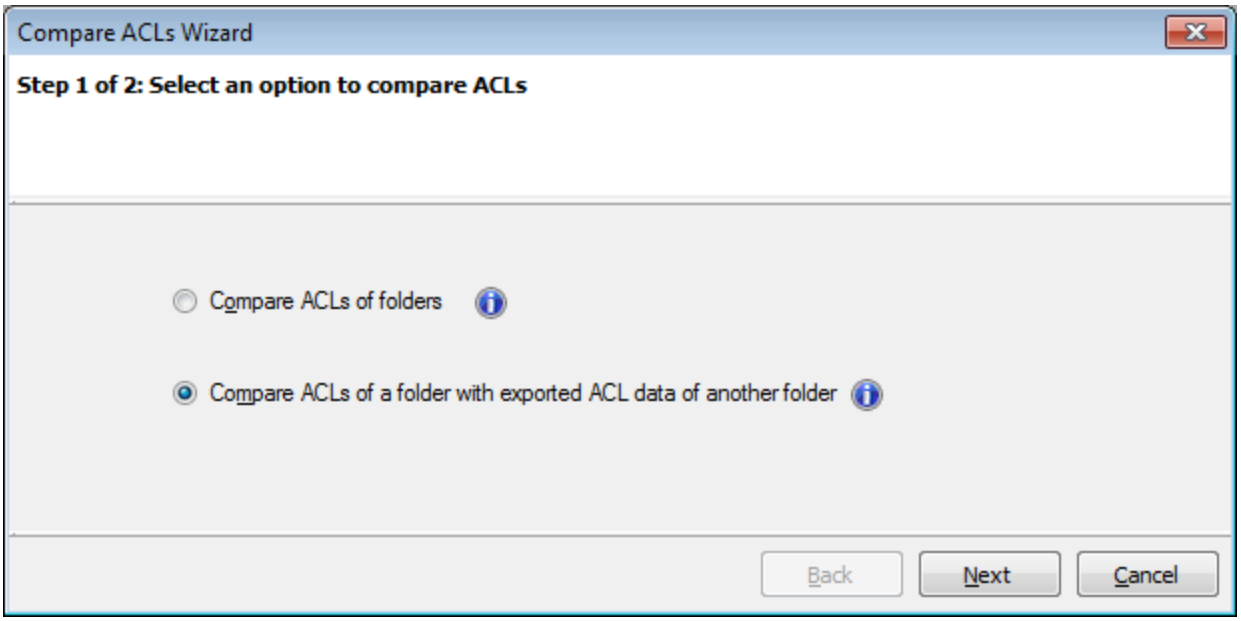
Click on 

button.

The Compare ACLs window will be displayed as shown below:

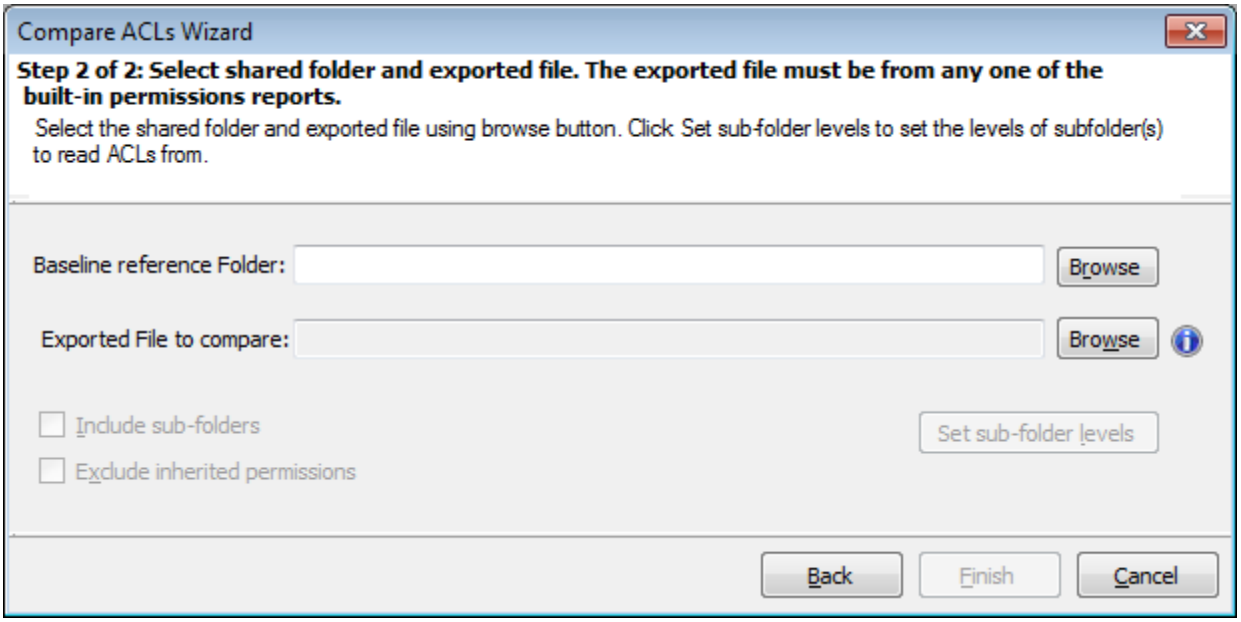
Step 1: Select an option to compare ACLs

Select **Compare ACLs of a folder with exported ACL data of another folder** option. Click **Next** to proceed to the Next step.


Compare ACLs Wizard
Step 1 of 2: Select an option to compare ACLs
Compare ACLs of folders
Compare ACLs of a folder with exported ACL data of another folder
Back
Next
Cancel

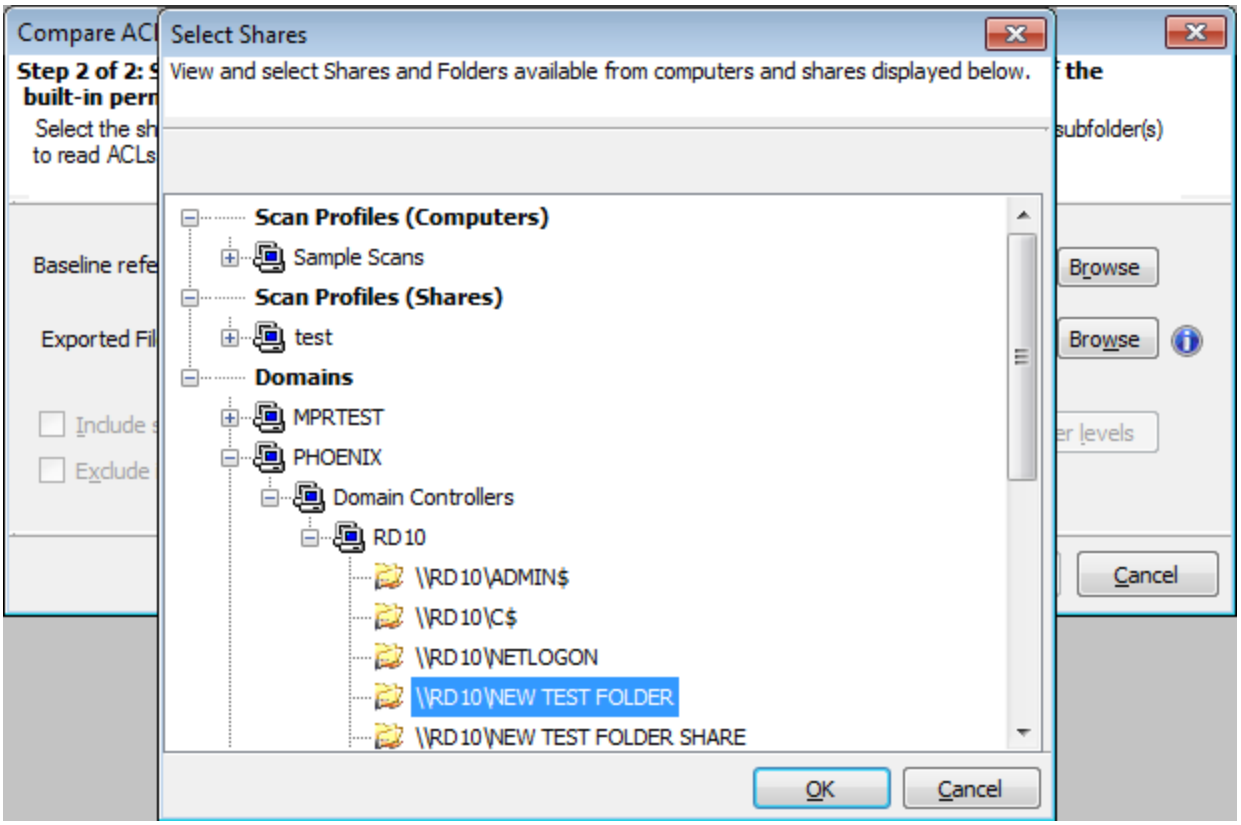
Step 2: Select shared folder and exported file. The exported file must be from any one of the built-in permissions reports.

Select a Baseline reference folder and a exported file to compare using the respective browse buttons.

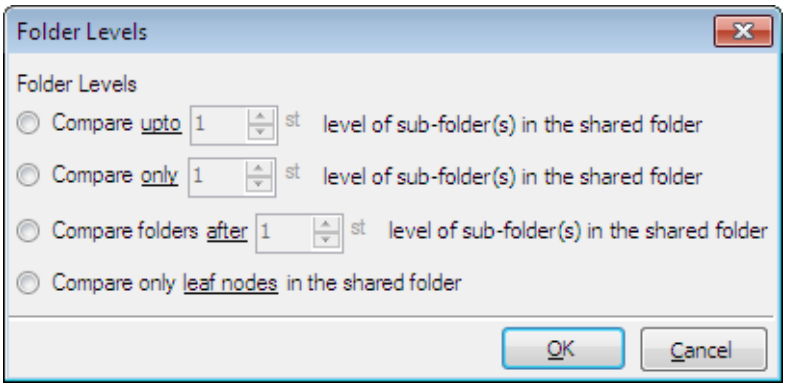

Compare ACLs Wizard
Step 2 of 2: Select shared folder and exported file. The exported file must be from any one of the built-in permissions reports.
Select the shared folder and exported file using browse button. Click Set sub-folder levels to set the levels of subfolder(s) to read ACLs from.
Baseline reference Folder:
Browse
Exported File to compare:
Browse
Include sub-folders
Set sub-folder levels
Exclude inherited permissions
Back
Finish
Cancel

Note: You may select an exported file of any one of the built-in permissions reports below:

- List of permissions for folders.
- List of permissions for specific users and groups on folders.
- List of permissions for files.
- List of permissions for specific users and groups on files.



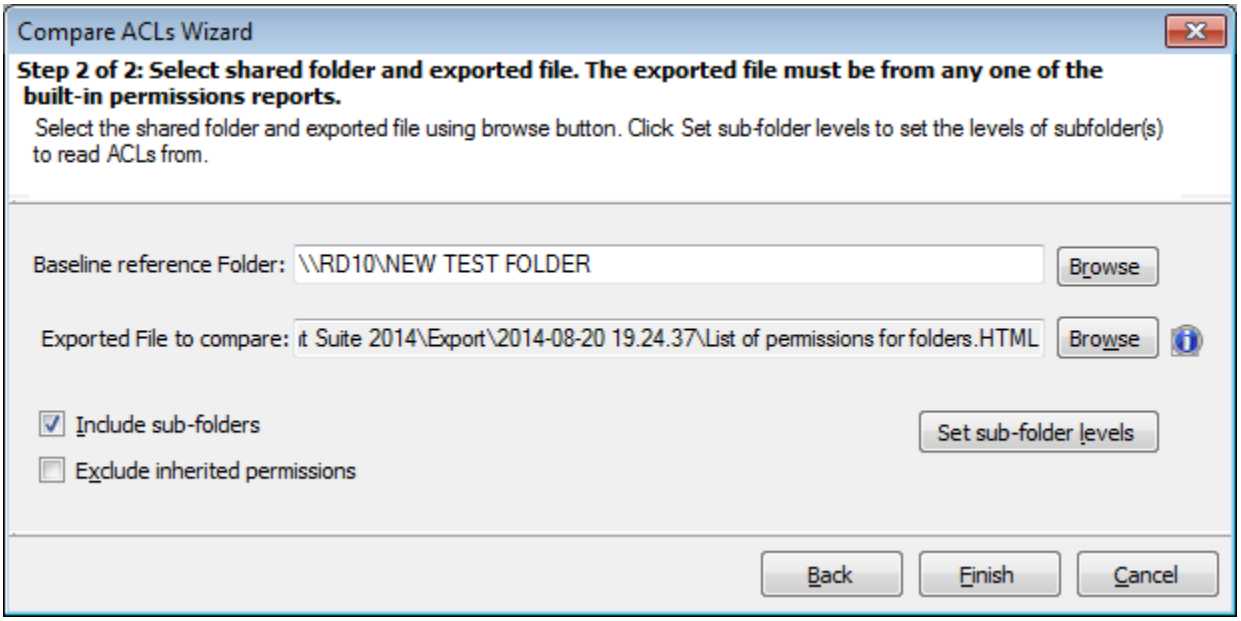
- **Include sub-folders**: Enabling this option will process the sub-folders of the specified shared folders for comparison.
- **Exclude inherited permissions**: Enabling this option will exclude inherited permissions of the specified shared folders for comparison.
- Use **Set sub-folder levels** to set the levels of subfolder(s) to read ACLs from.


Folder Levels
Folder Levels
Compare upto 1 st level of sub-folder(s) in the shared folder
Compare only 1 st level of sub-folder(s) in the shared folder
Compare folders after 1 st level of sub-folder(s) in the shared folder
Compare only leaf nodes in the shared folder
OK
Cancel

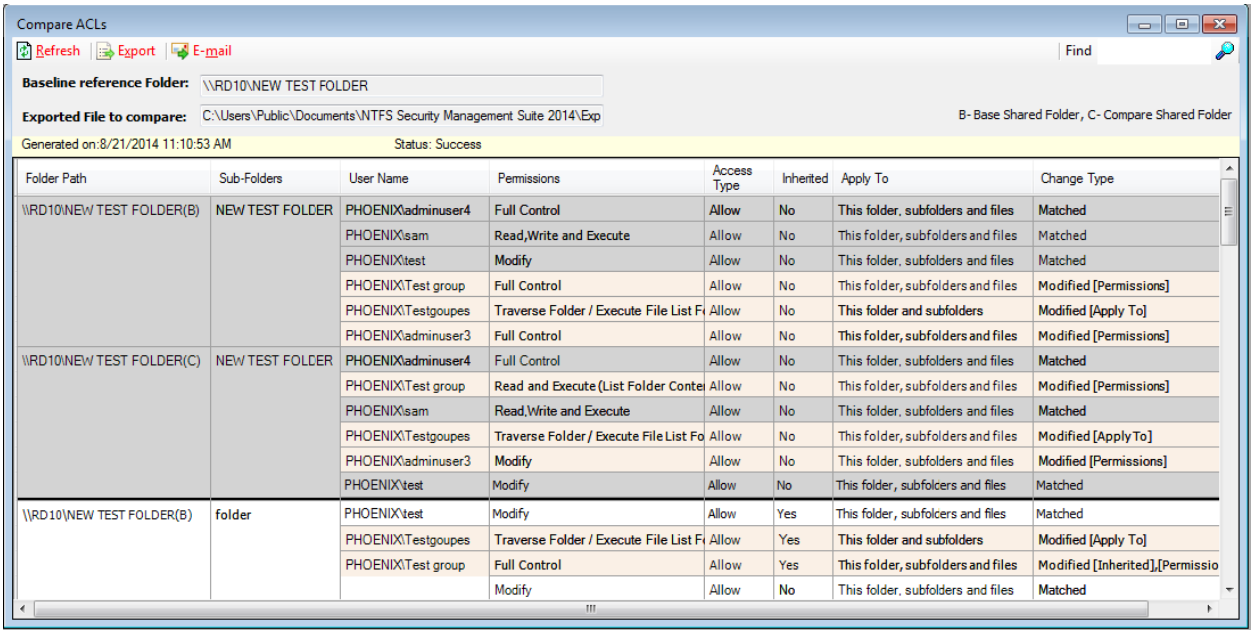
The Sub-folder levels window allows the user to specify the option to enumerate sub-folders for comparing their ACLs, as stated below:

- Compare upto N level(s) of sub-folder(s) in the shared folders: This option will take selected shared folder of sub-folders which are upto the specified traversal level and compare ACLs only those named sub-folders that are common to the selected shared folder and exported shared folder report.

- Compare only Nth level of sub-folder(s) in the shared folders: This option will take selected shared folder of sub-folders which are in the specified folder level only and compare ACLs only those named sub-folders that are common to the selected shared folder and exported shared folder report.
- Compare folders after N level(s) of sub-folder(s) in the shared folders: This option will take selected shared folder of sub-folders which are after the nth folder level and compare ACLs only those name sub-folders that are common to the selected shared folder and exported shared folder report.
- Compare only leaf nodes in the shared folders: This option will take selected shared folder of last child (leaf) nodes of sub-folders and compare ACLs only those name sub-folders that are common to the selected shared folder and exported shared folder report.


Compare ACLs Wizard
Step 2 of 2: Select shared folder and exported file. The exported file must be from any one of the built-in permissions reports.
Select the shared folder and exported file using browse button. Click Set sub-folder levels to set the levels of subfolder(s) to read ACLs from.
Baseline reference Folder:
\\RD10\NEW TEST FOLDER
Browse
Exported File to compare:
it Suite 2014\Export\2014-08-20 19.24.37\List of permissions for folders.HTML
Browse
Include sub-folders
Set sub-folder levels
Exclude inherited permissions
Back
Finish
Cancel

Click **Finish** to generate the compared ACLs report.



Folder Path	Sub-Folders	User Name	Permissions	Access Type	Inherited	Apply To	Change Type
\\RD10\NEW TEST FOLDER(B)	NEW TEST FOLDER	PHOENIX\adminuser4	Full Control	Allow	No	This folder, subfolders and files	Matched
		PHOENIX\sam	Read,Write and Execute	Allow	No	This folder, subfolders and files	Matched
		PHOENIX\test	Modify	Allow	No	This folder, subfolders and files	Matched
		PHOENIX\Test group	Full Control	Allow	No	This folder, subfolders and files	Modified [Permissions]
		PHOENIX\Testgoupes	Traverse Folder / Execute File List F	Allow	No	This folder and subfolders	Modified [Apply To]
		PHOENIX\adminuser3	Full Control	Allow	No	This folder, subfolders and files	Modified [Permissions]
\\RD10\NEW TEST FOLDER(C)	NEW TEST FOLDER	PHOENIX\adminuser4	Full Control	Allow	No	This folder, subfolders and files	Matched
		PHOENIX\Test group	Read and Execute (List Folder Conte	Allow	No	This folder, subfolders and files	Modified [Permissions]
		PHOENIX\sam	Read,Write and Execute	Allow	No	This folder, subfolders and files	Matched
		PHOENIX\Testgoupes	Traverse Folder / Execute File List Fo	Allow	No	This folder, subfolders and files	Modified [Apply To]
		PHOENIX\adminuser3	Modify	Allow	No	This folder, subfolders and files	Modified [Permissions]
		PHOENIX\test	Modify	Allow	No	This folder, subfolcers and files	Matched
\\RD10\NEW TEST FOLDER(B)	folder	PHOENIX\test	Modify	Allow	Yes	This folder, subfolcers and files	Matched
		PHOENIX\Testgoupes	Traverse Folder / Execute File List F	Allow	Yes	This folder and subfolders	Modified [Apply To]
		PHOENIX\Test group	Full Control	Allow	Yes	This folder, subfolders and files	Modified [Inherited],[Permissio
			Modify	Allow	No	This folder, subfolders and files	Matched

Security Vulnerabilities

How to view Security Vulnerabilities Reports?

How to view Security Vulnerabilities Reports?

Security Vulnerabilities Reports provides reports that focus solely on reporting the vulnerabilities access permissions assigned to user and groups on shared folder(s)/file(s).

Click on

button.

List of Security Vulnerabilities Reports:

List of all explicit permissions for folders

List of folders with broken inheritance and their permissions

List of permissions for orphaned accounts on folders

List of permissions for disabled user accounts on folders

List of permissions for having destructive access on folders

List of folders that have Deny permissions set (both Explicit and Inherited)

List of user accounts that have indirect access to folders due to nested group membership

List of Effective access for specific users and groups on folders

List of folders that have permissions for 'Everyone' group

List of all explicit permissions for folders

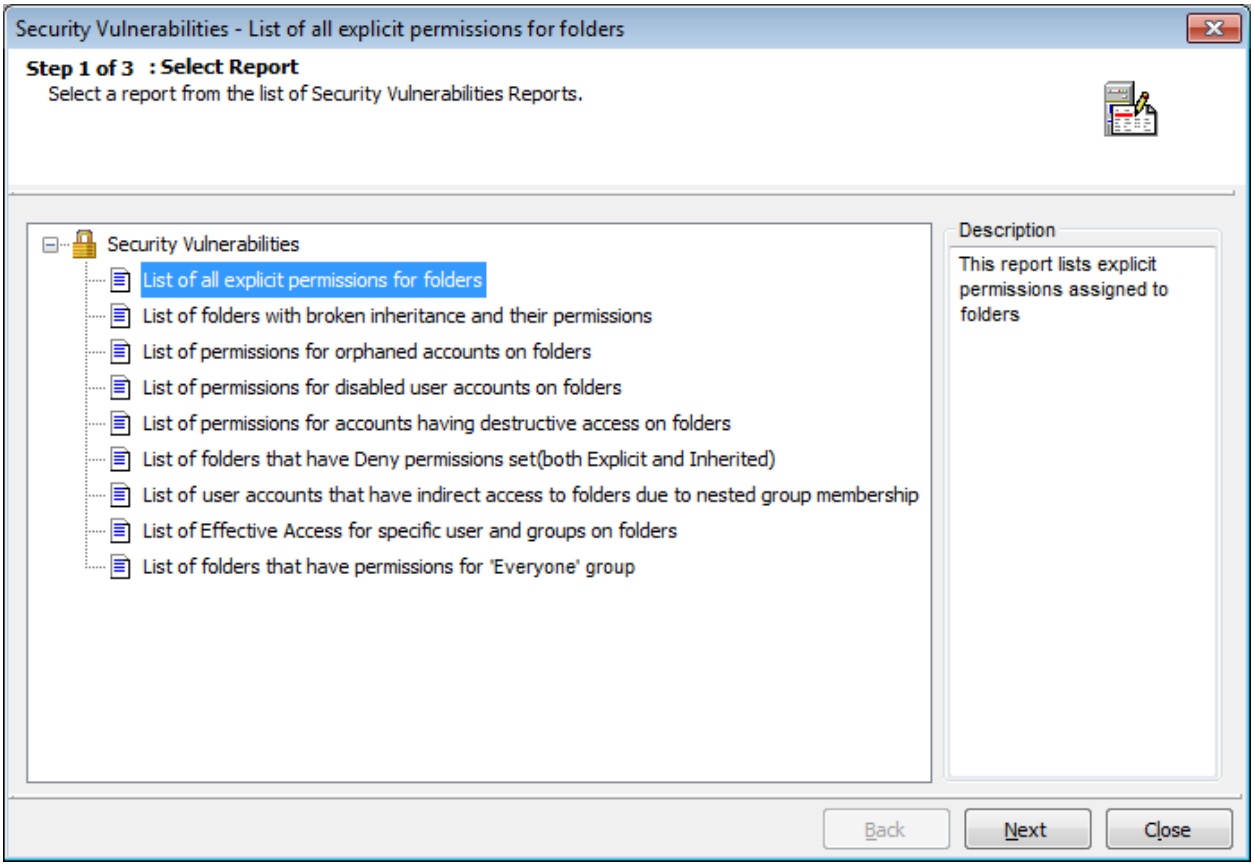
This report allows you to view explicit permissions assigned to folders.

Click on

button.

Step 1: Report Selection

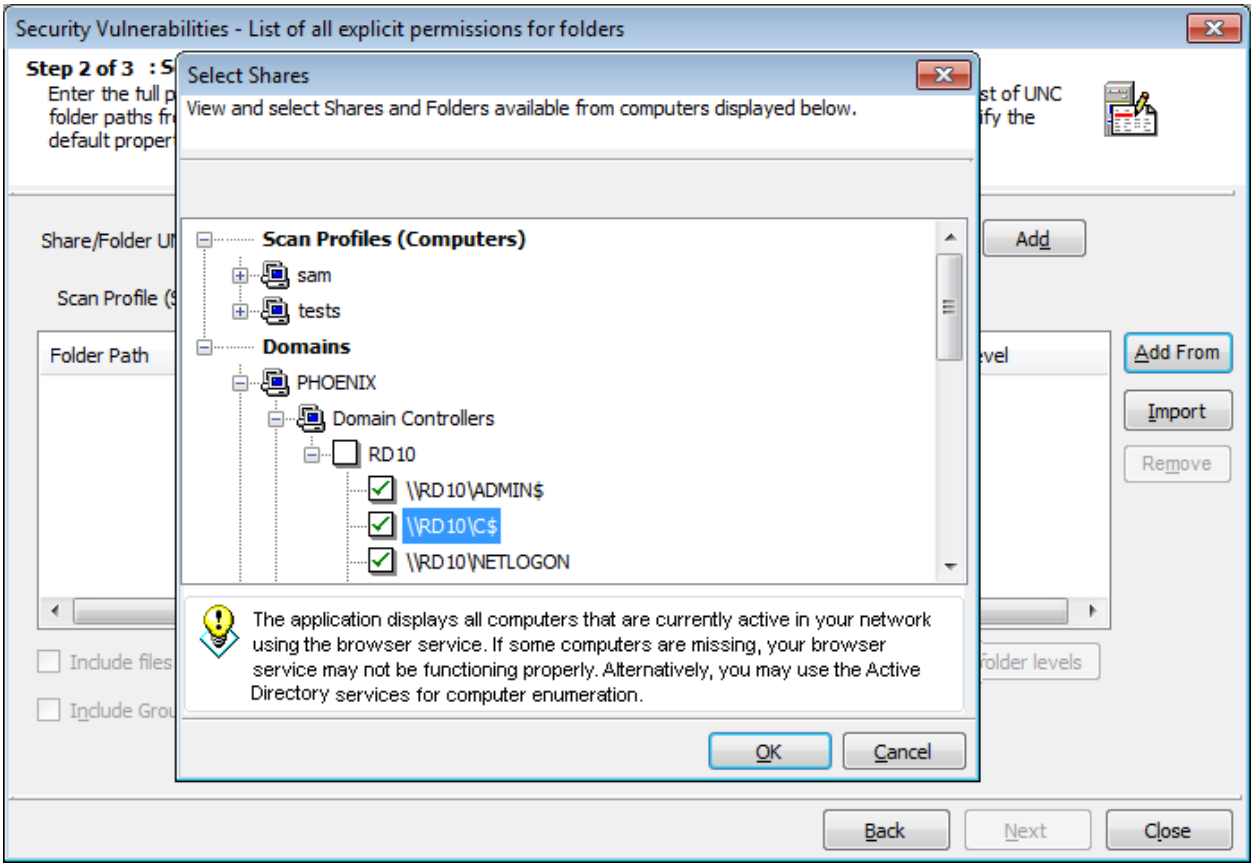
Select the report to be generated. Only one report can be generated at a time.

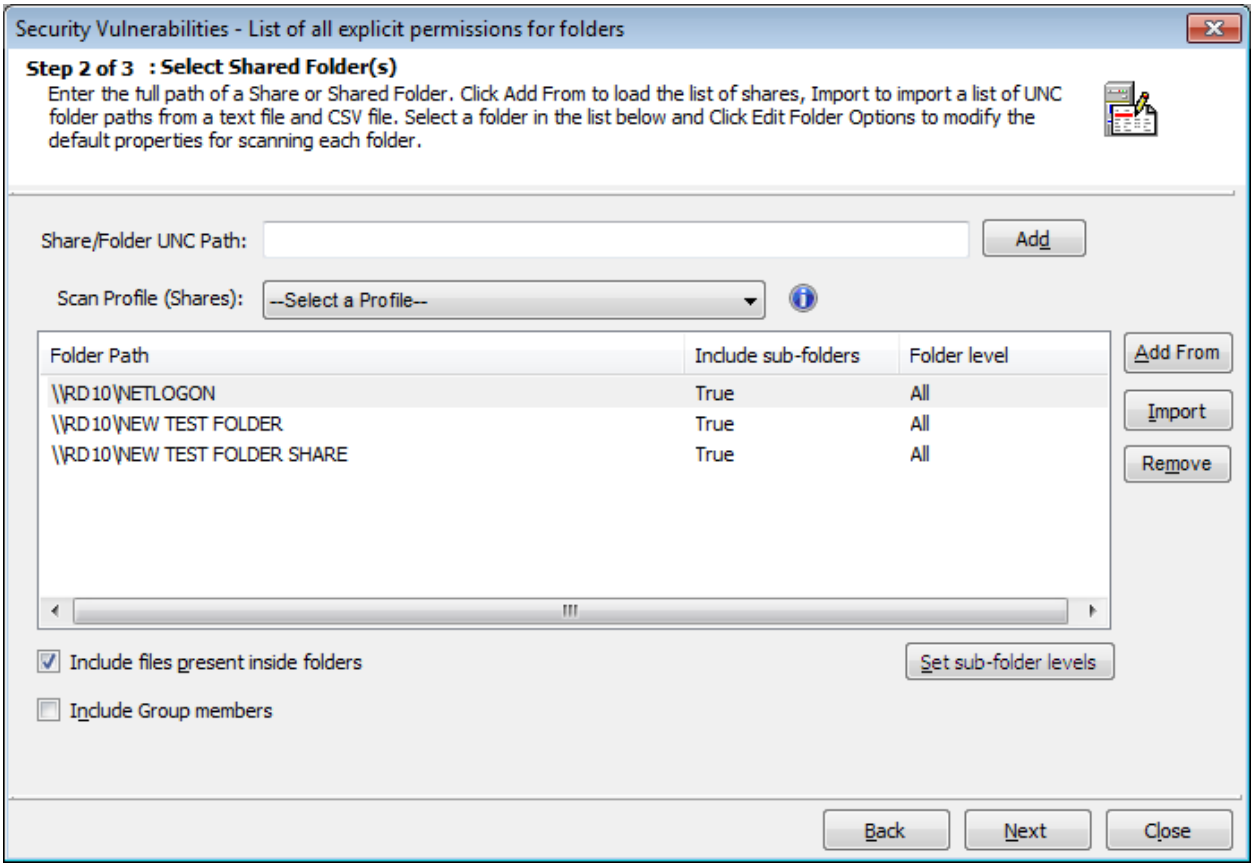

Security Vulnerabilities - List of all explicit permissions for folders
Step 1 of 3 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists explicit permissions assigned to folders
Back
Next
Close

Click Next to proceed to the next step.

Step 2: Select shared folders:

Select one or more servers to retrieve available shares


Security Vulnerabilities - List of all explicit permissions for folders
Step 2 of 3 : S
Enter the full p
folder paths fr
default proper
st of UNC
ify the
Share/Folder UI
Scan Profile (S
Folder Path
Add
Add From
Import
Remove
Include files
Include Grou
folder levels
Back
Next
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel

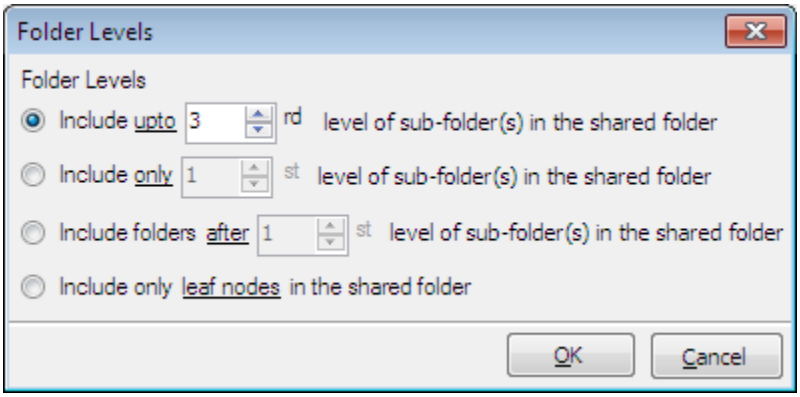

Security Vulnerabilities - List of all explicit permissions for folders
Step 2 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Include Group members
Back
Next
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

You can select Include Group members option to include all the members of a group and their sub-group members at all group levels in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

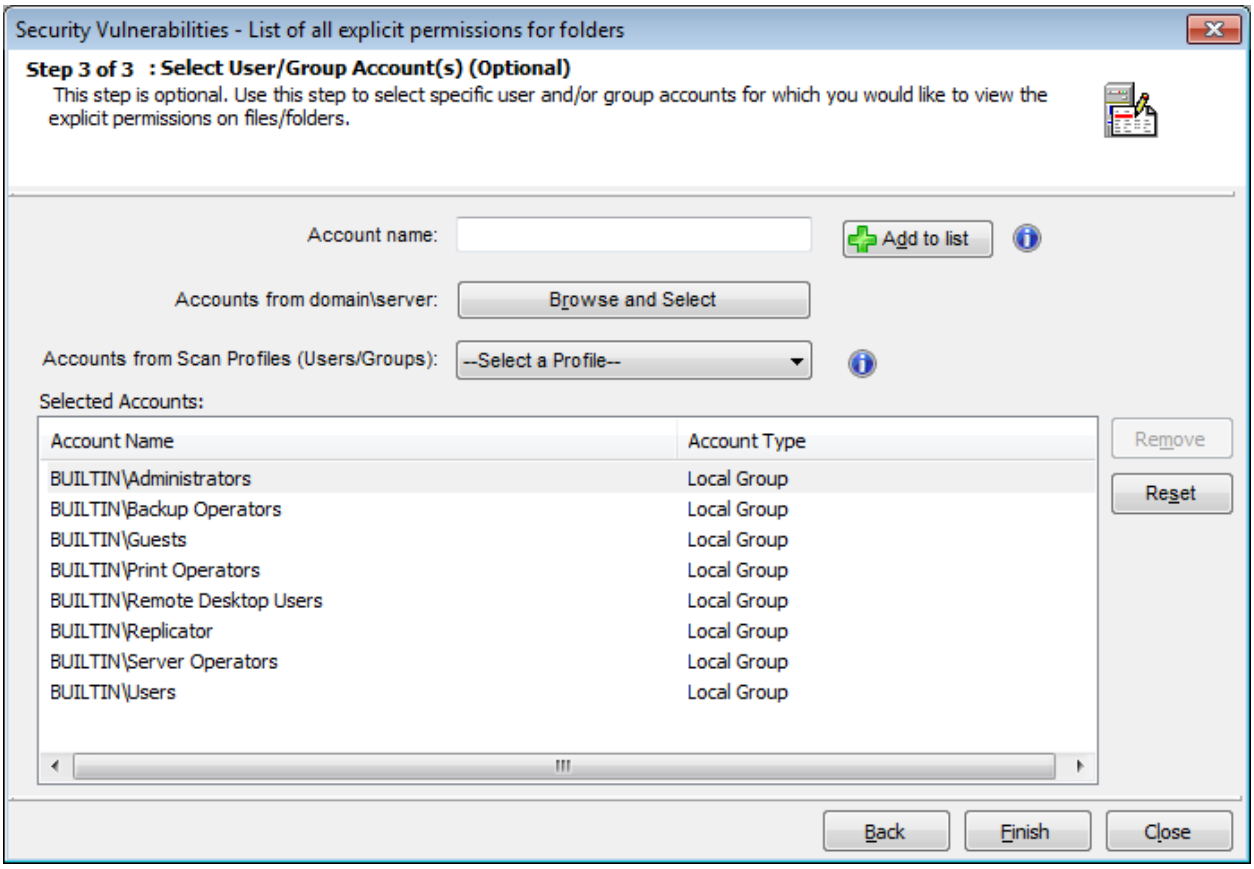
Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Next** to proceed to the next step.

Step 3: Select User/Group Accounts:

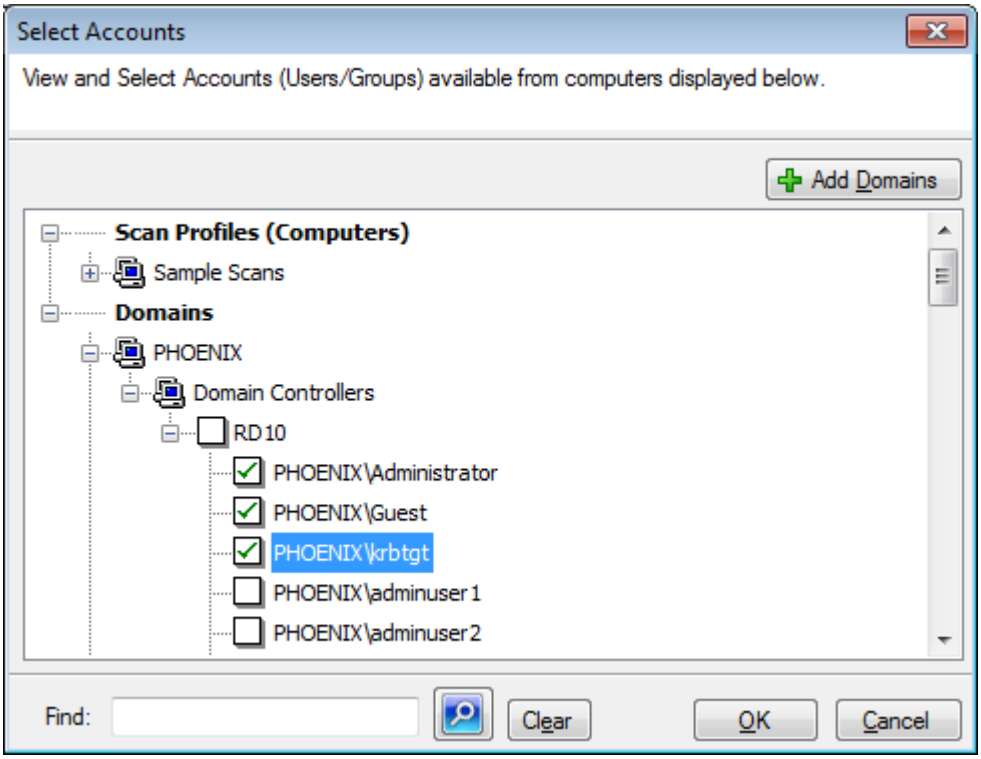
This step is optional. Use this step to select user and/or group accounts for which you like to view the explicit permissions for folders/files.



Enter User/Group name in domain\account name format and click Add to List to add the user/group to the selected accounts list

Use Select a Scan Profile (Users/Groups) option to use the users and groups added in a profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

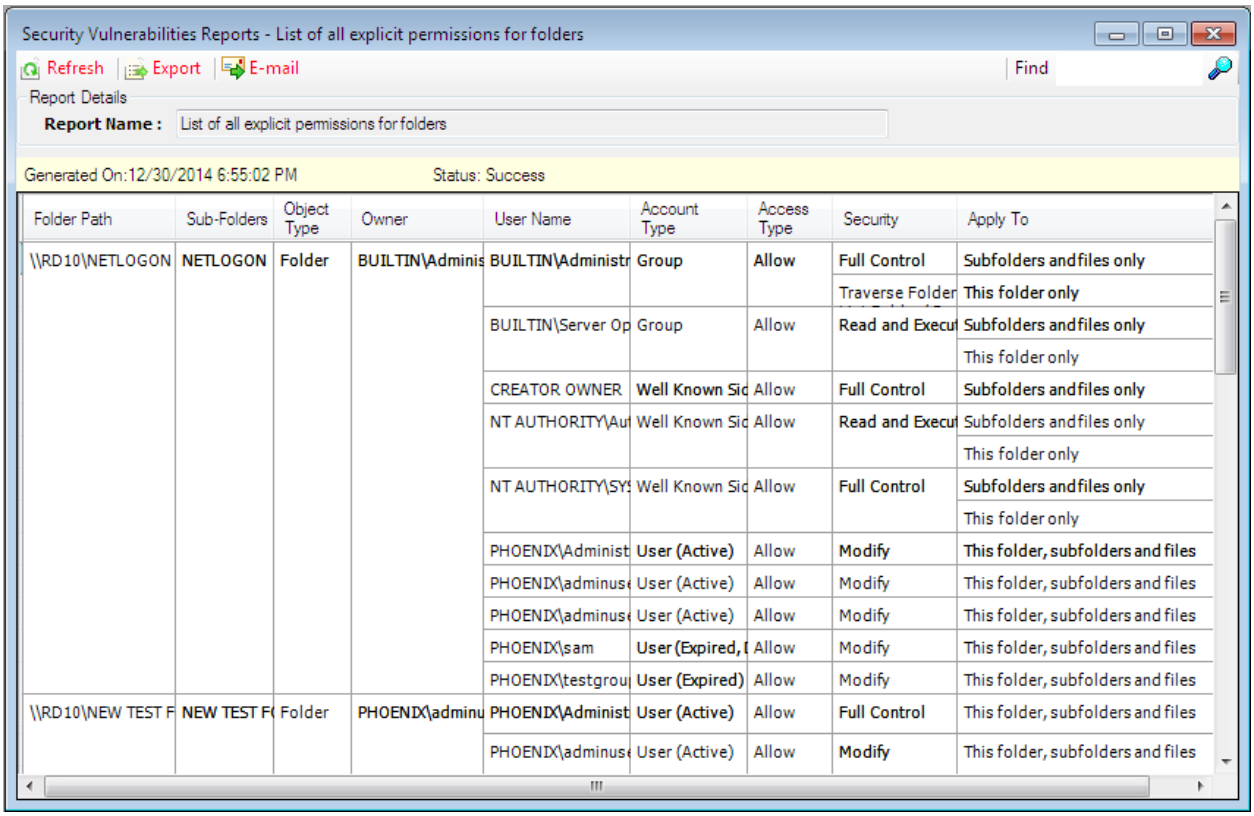
Use Browse and Select option to retrieve users and groups from servers or Scan Profile (Computers).



Use the Find option to search desired user/group accounts.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



Folder Path	Sub-Folders	Object Type	Owner	User Name	Account Type	Access Type	Security	Apply To
\\RD10\NETLOGON	NETLOGON	Folder	BUILTIN\Adminis	BUILTIN\Administr	Group	Allow	Full Control	Subfolders and files only
							Traverse Folder	This folder only
				BUILTIN\Server Op	Group	Allow	Read and Execut	Subfolders and files only
								This folder only
				CREATOR OWNER	Well Known Sid	Allow	Full Control	Subfolders and files only
				NT AUTHORITY\Aut	Well Known Sid	Allow	Read and Execut	Subfolders and files only
								This folder only
				NT AUTHORITY\SY	Well Known Sid	Allow	Full Control	Subfolders and files only
								This folder only
				PHOENIX\Administ	User (Active)	Allow	Modify	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	Modify	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	Modify	This folder, subfolders and files
				PHOENIX\sam	User (Expired,	Allow	Modify	This folder, subfolders and files
				PHOENIX\testgrou	User (Expired)	Allow	Modify	This folder, subfolders and files
\\RD10\NEW TEST F	NEW TEST F	Folder	PHOENIX\adminu	PHOENIX\Administ	User (Active)	Allow	Full Control	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	Modify	This folder, subfolders and files

List of folders with broken inheritance and their permissions

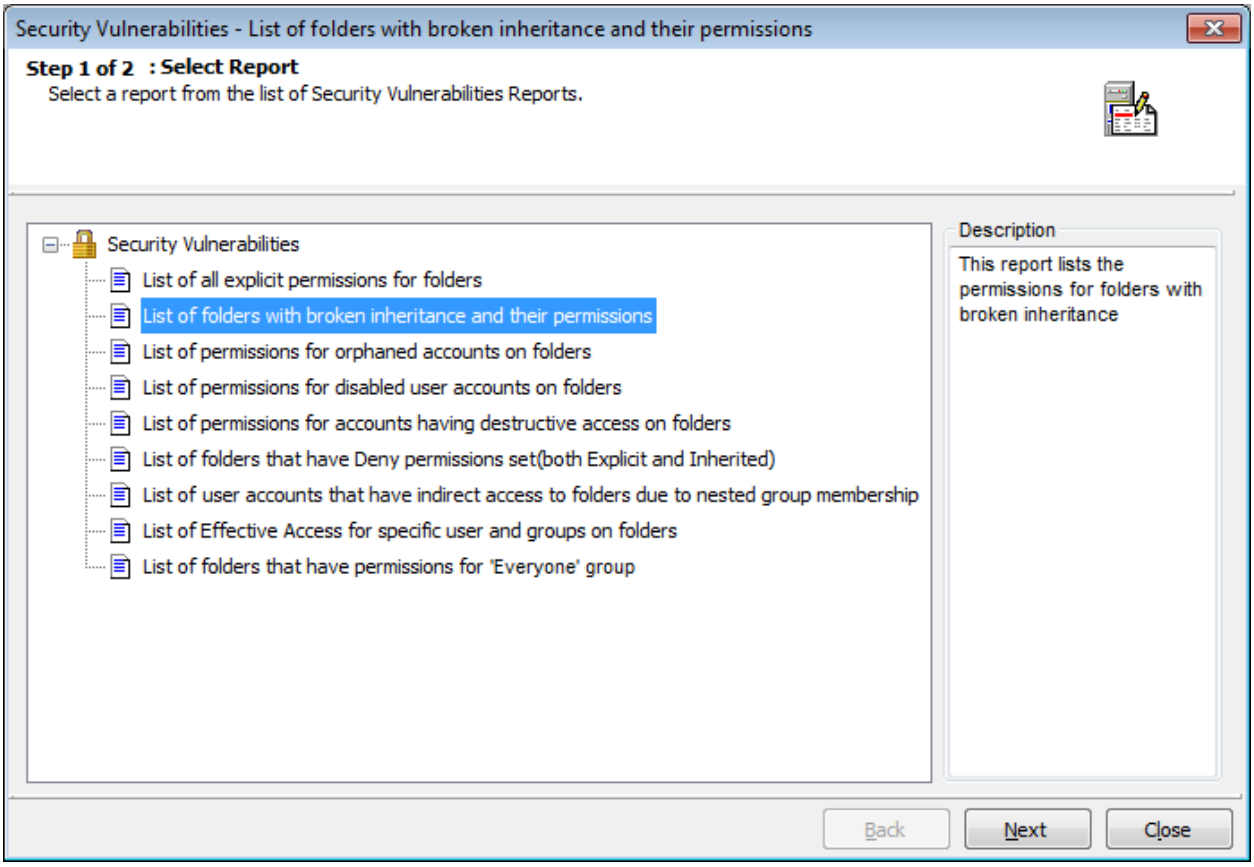
This report allows you to view the list of folders where inheritance is broken and the assigned permissions.

Click on

button.

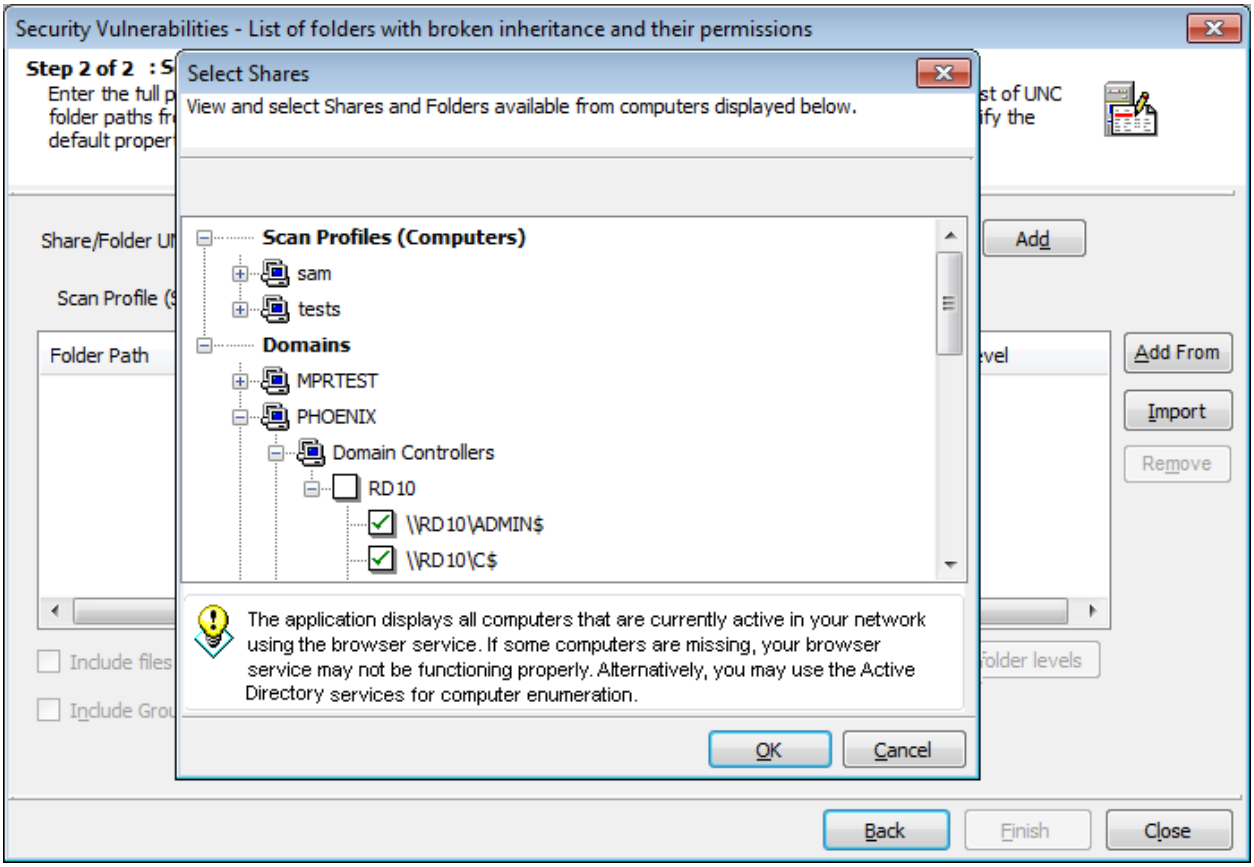
Step 1: Report Selection

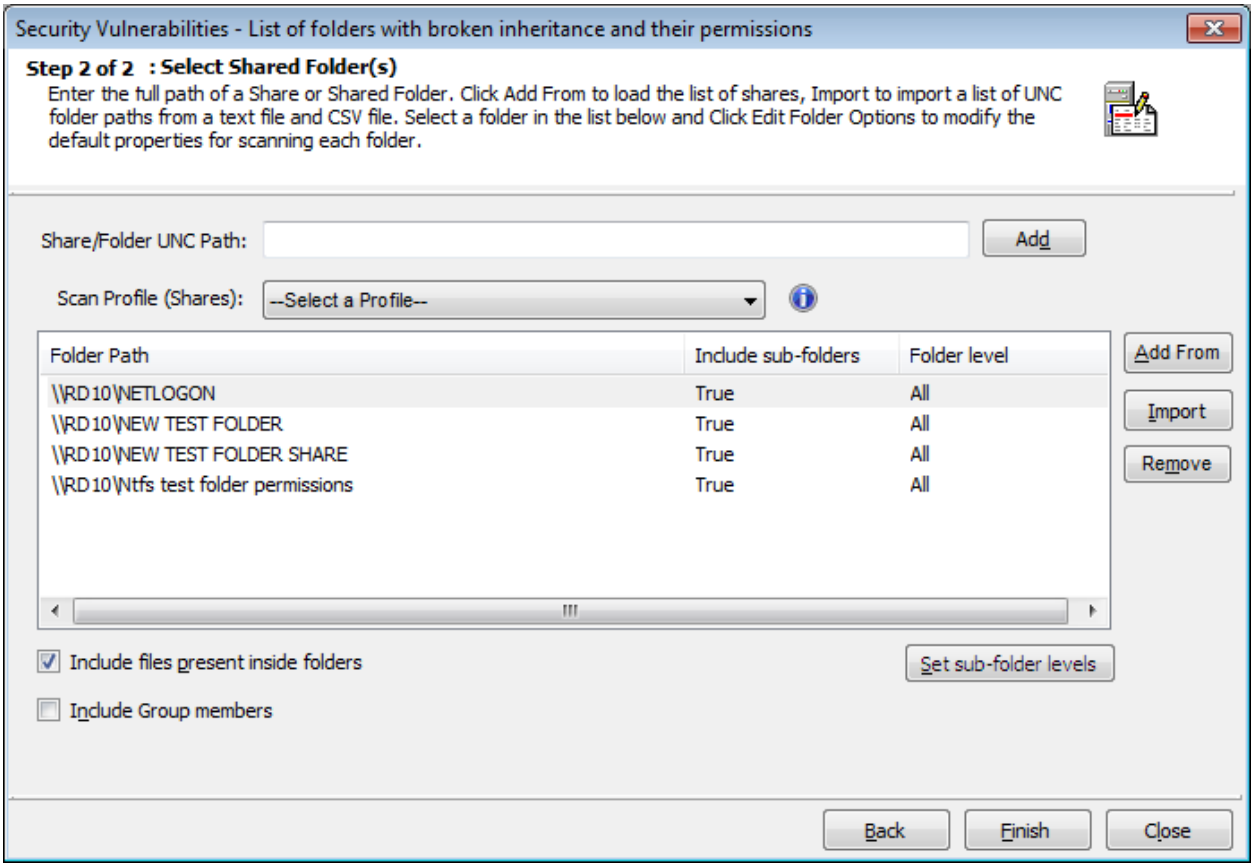
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of folders with broken inheritance and their permissions
Step 1 of 2 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists the permissions for folders with broken inheritance
Back
Next
Close

Step 2: Select shared folders

Select one or more servers to retrieve available shares.


Security Vulnerabilities - List of folders with broken inheritance and their permissions
Step 2 of 2 : S
Enter the full p
folder paths fr
default proper
st of UNC
ify the
Share/Folder UI
Scan Profile (S
Add
Folder Path
Add From
Import
Remove
Include files
Include Grou
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel

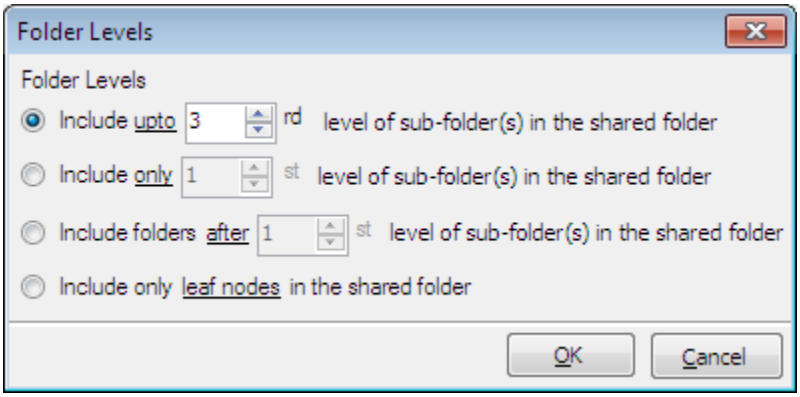

Security Vulnerabilities - List of folders with broken inheritance and their permissions
Step 2 of 2 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Include Group members
Back
Finish
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

You can select Include Group members option to include all the members of a group and their sub-group members at all group levels in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

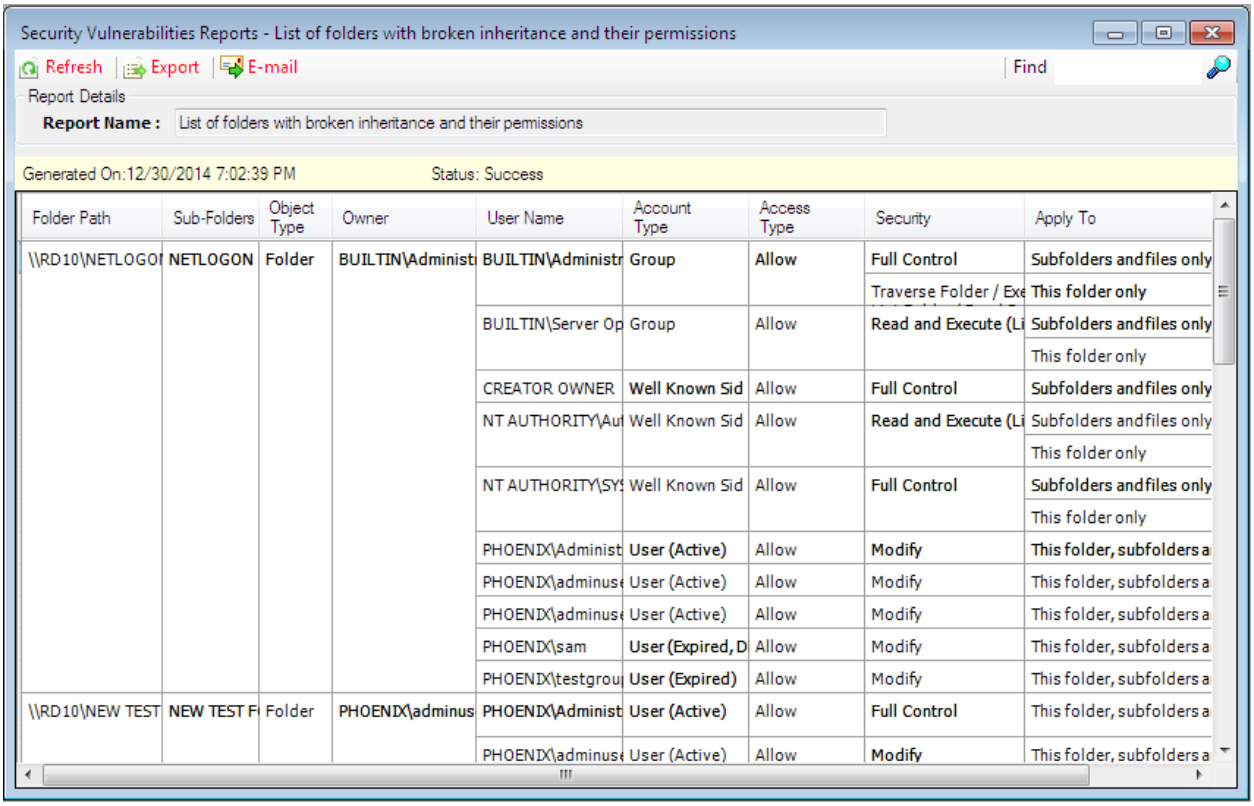
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



List of permissions for orphaned accounts on folders

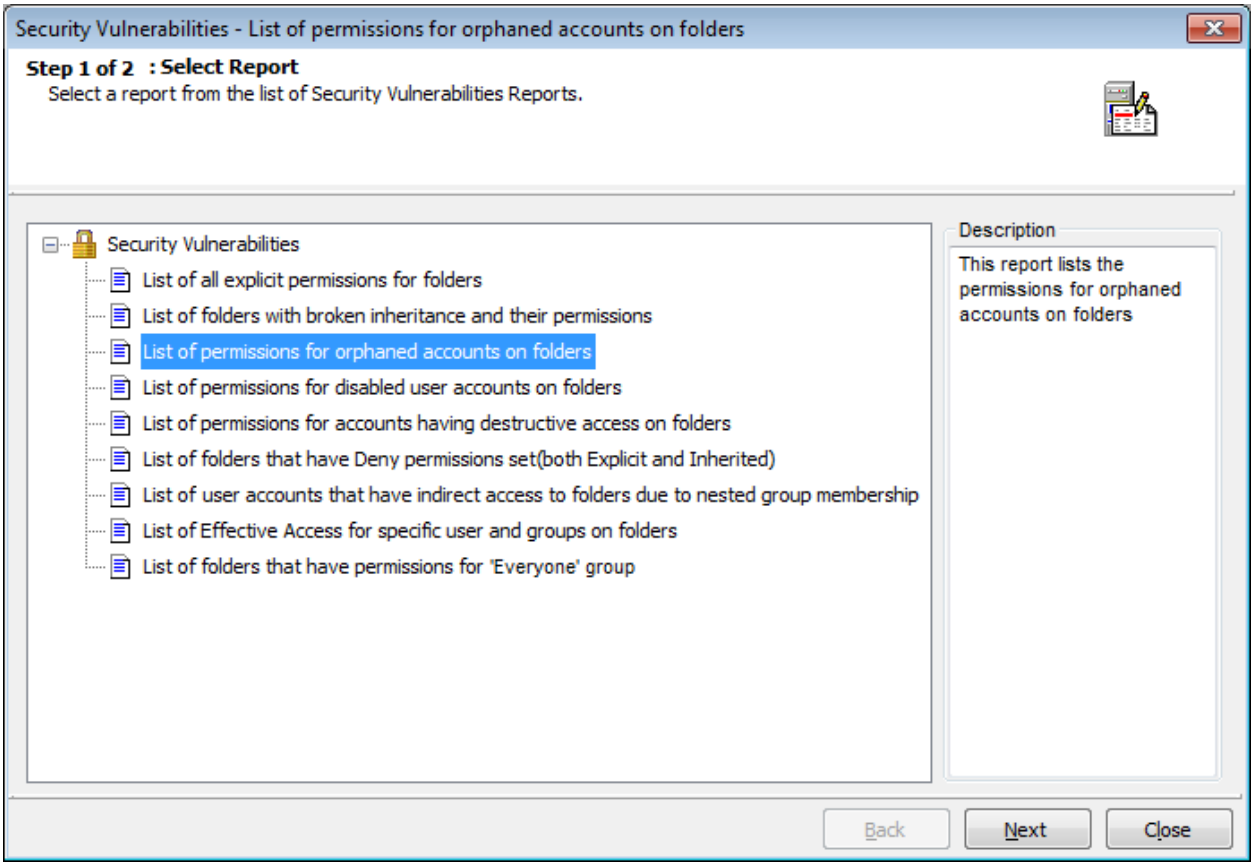
This report allows you to view the permissions for orphaned accounts on folders.

Click on

button.

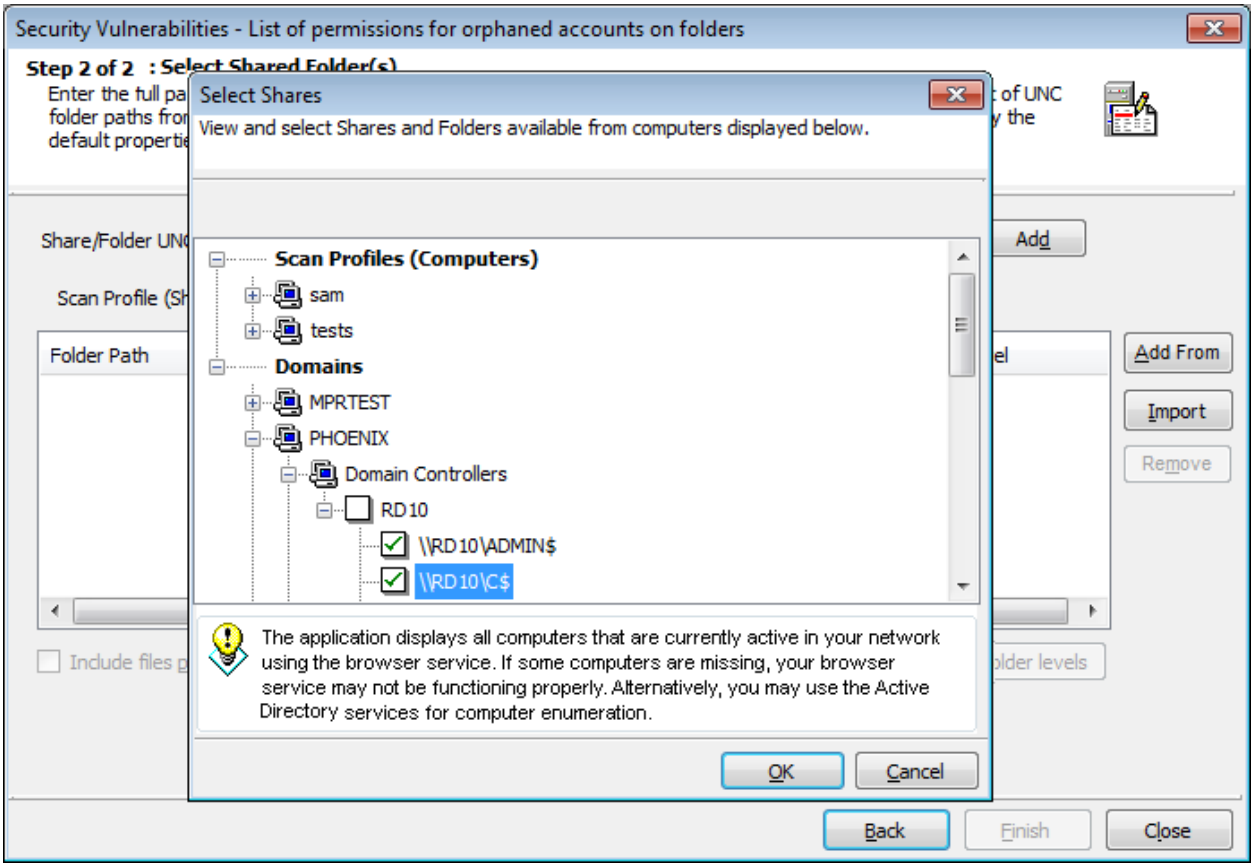
Step 1: Report Selection

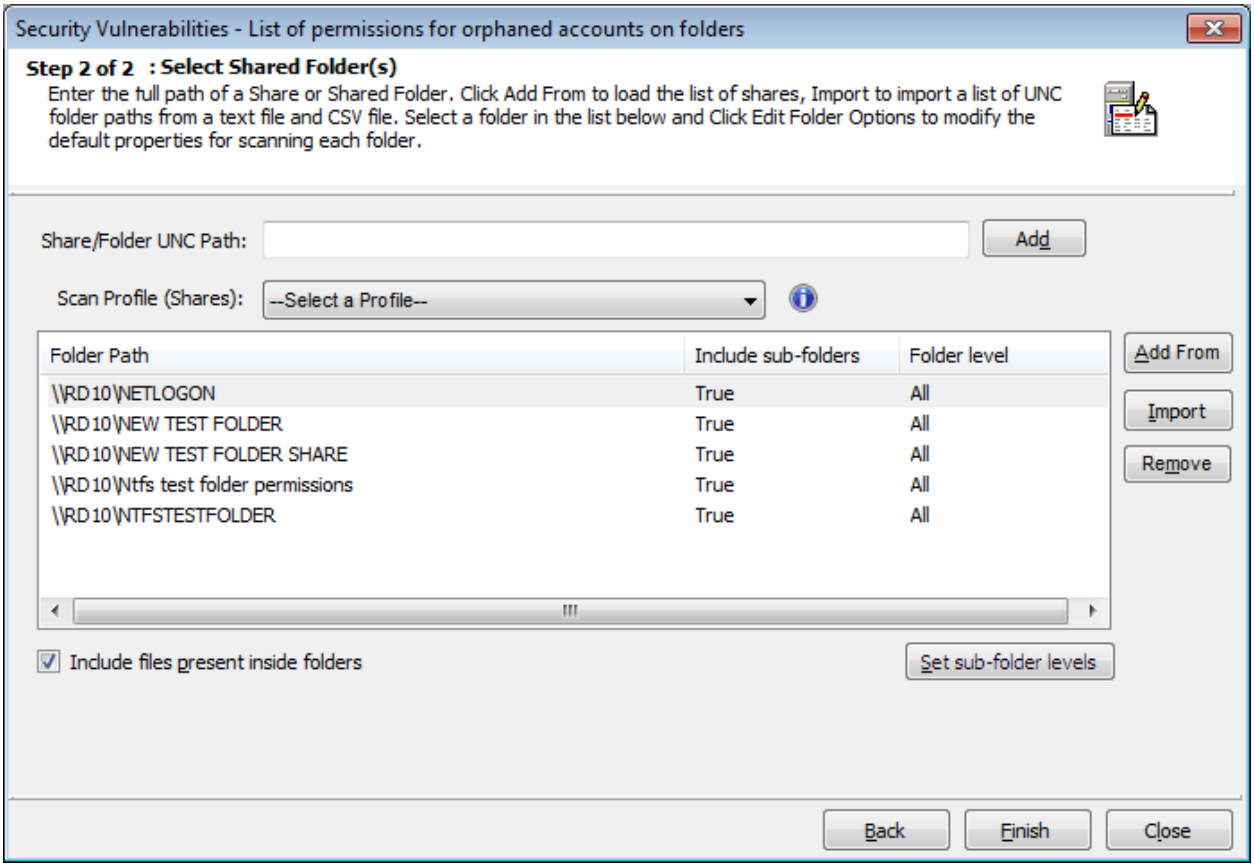
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of permissions for orphaned accounts on folders
Step 1 of 2 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists the permissions for orphaned accounts on folders
Back
Next
Close

Step 2: Select shared folders

Select one or more servers to retrieve available shares.

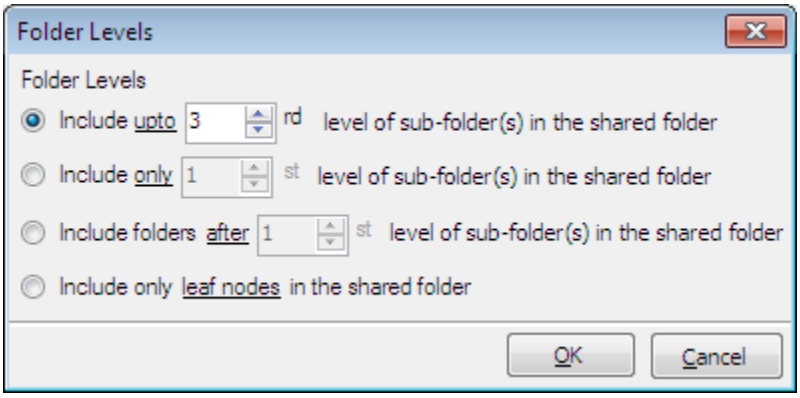

Security Vulnerabilities - List of permissions for orphaned accounts on folders
Step 2 of 2 : Select Shared Folder(s)
Enter the full pa
folder paths fro
default propertie
of UNC
y the
Share/Folder UN
Scan Profile (SH
Folder Path
Add
Add From
Import
Remove
Include files
older levels
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel



You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

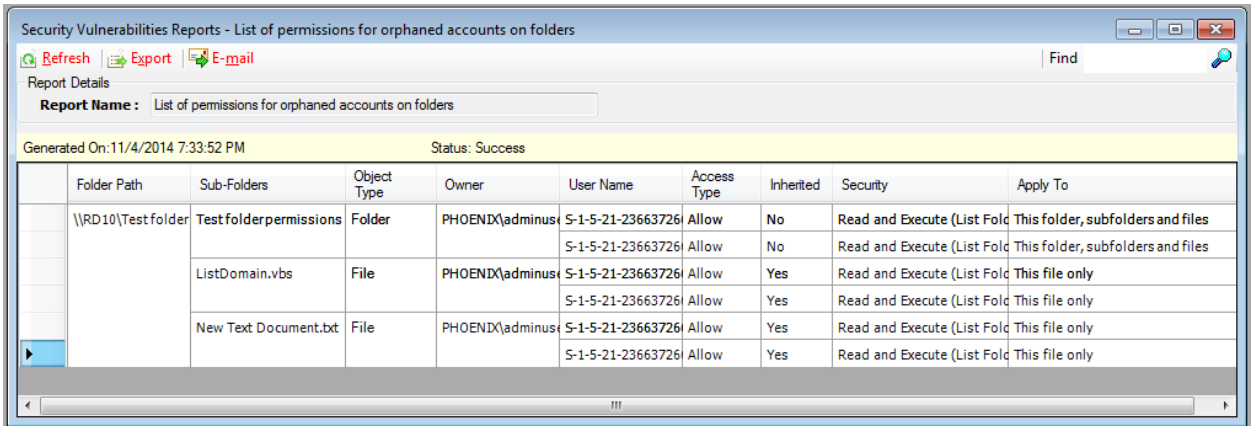
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



List of permissions for disabled user accounts on folders

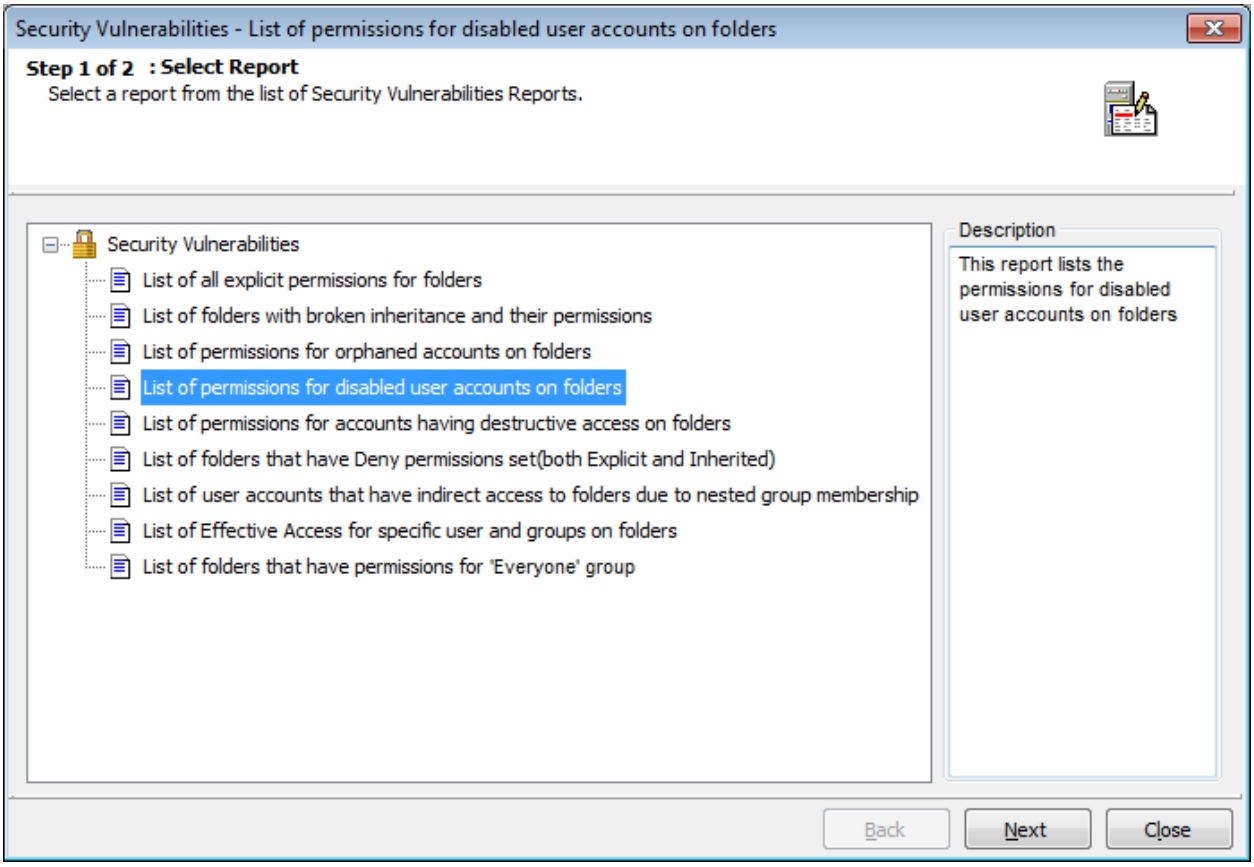
This report allows you to view the permissions for disabled user accounts on folders.

Click on

button.

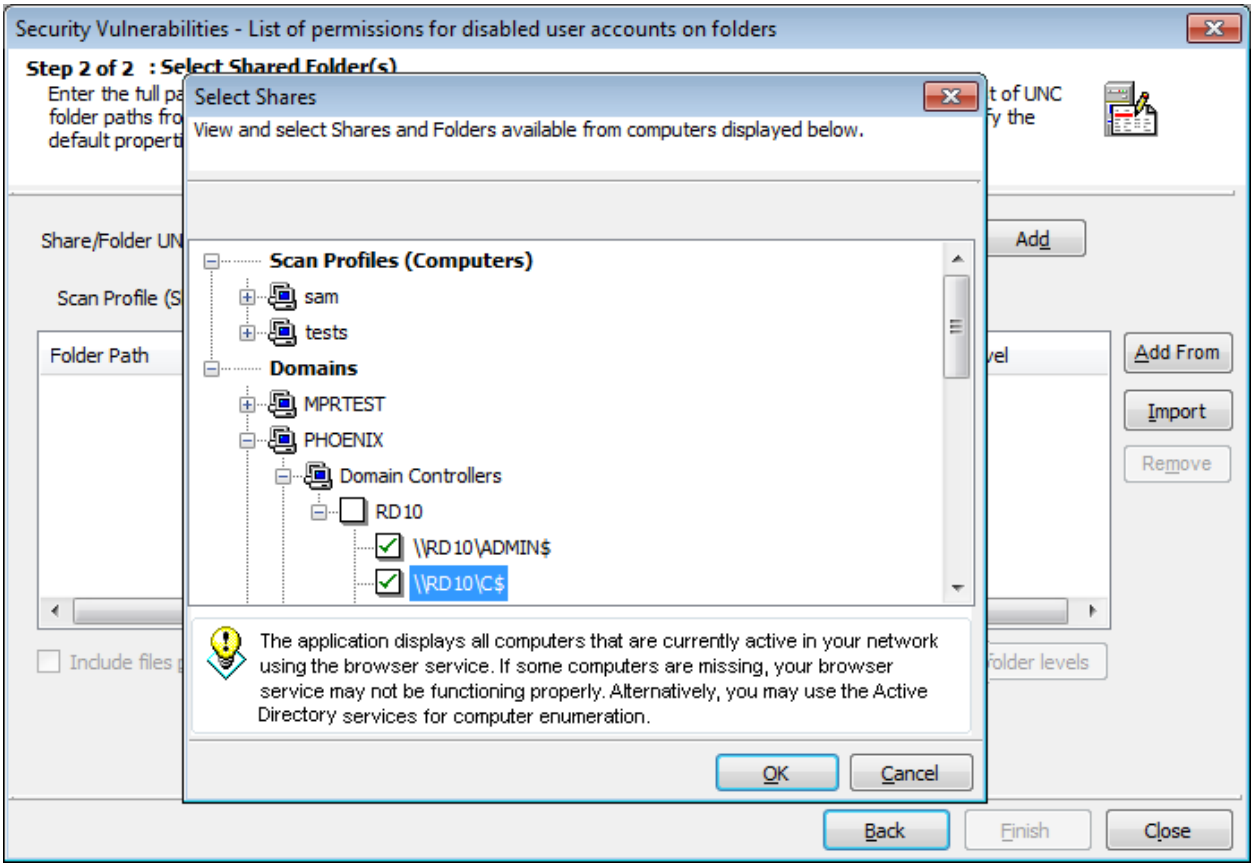
Step 1: Report Selection

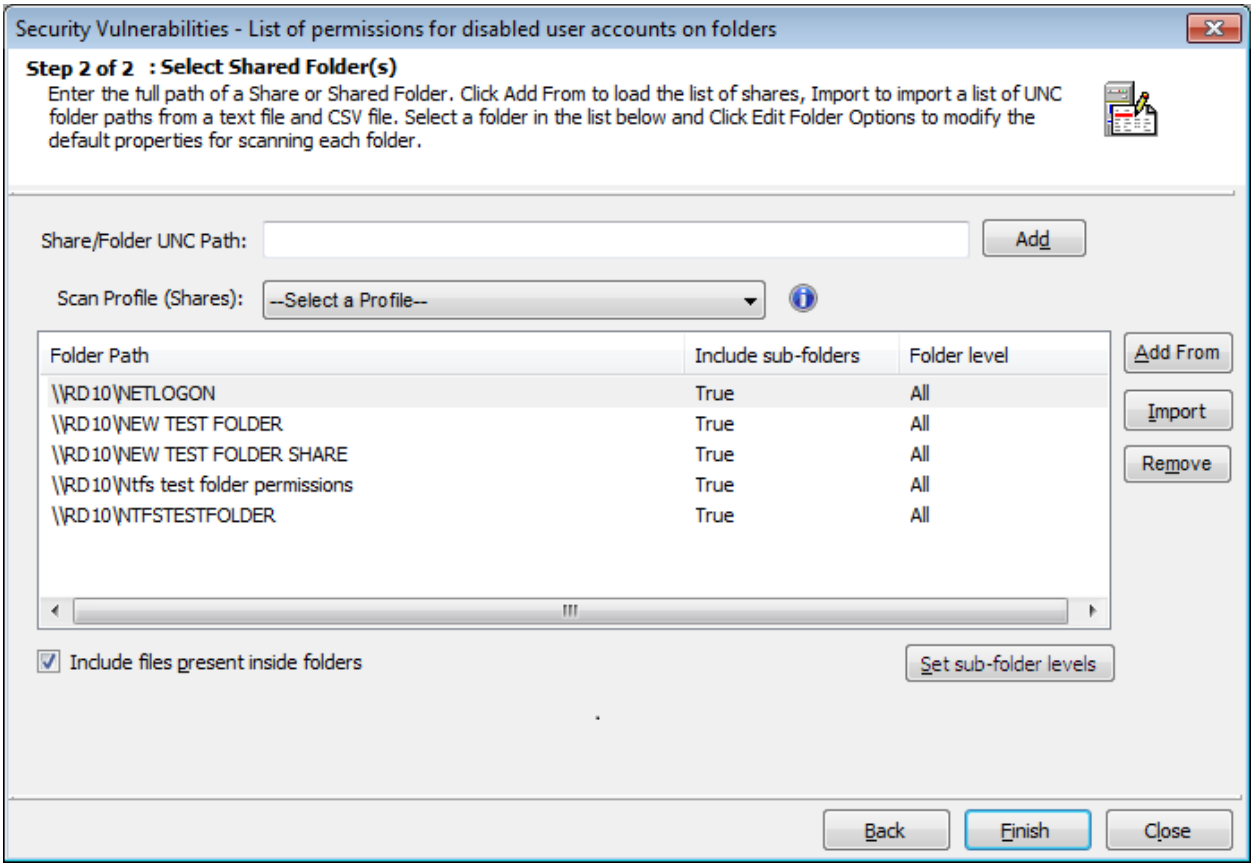
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of permissions for disabled user accounts on folders
Step 1 of 2 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists the permissions for disabled user accounts on folders
Back
Next
Close

Step 2: Select shared folders

Select one or more servers to retrieve available shares.

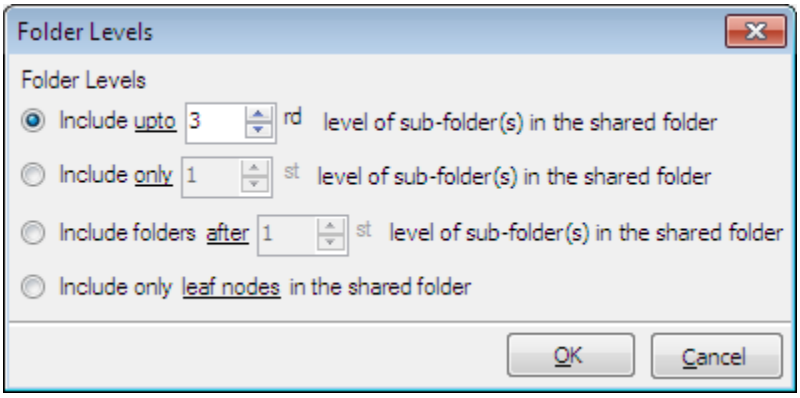

Security Vulnerabilities - List of permissions for disabled user accounts on folders
Step 2 of 2 : Select Shared Folder(s)
Enter the full pa
folder paths fro
default propert
t of UNC
y the
Share/Folder UN
Add
Scan Profile (S
Folder Path
Add From
Import
Remove
Include files
Folder levels
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel



You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

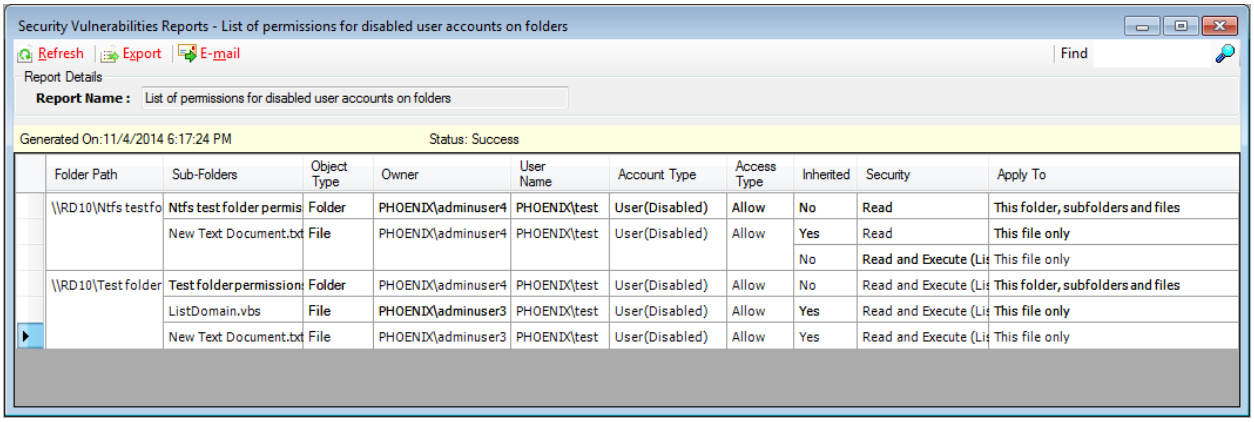
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



List of permissions for accounts having destructive access on folders

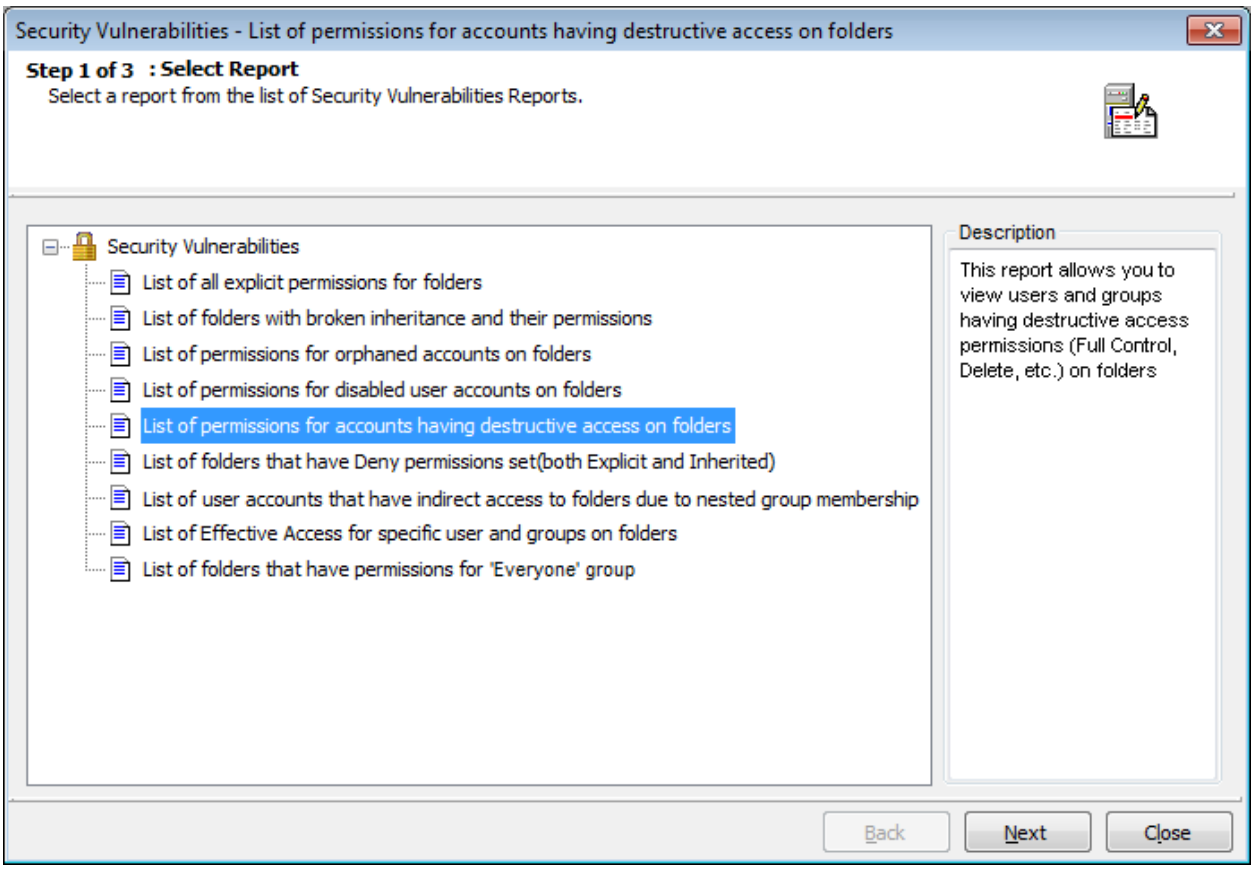
This report allows you to view users and groups having destructive access permissions (Full Control, Delete etc.) on folders.

Click on

button.

Step 1: Report Selection

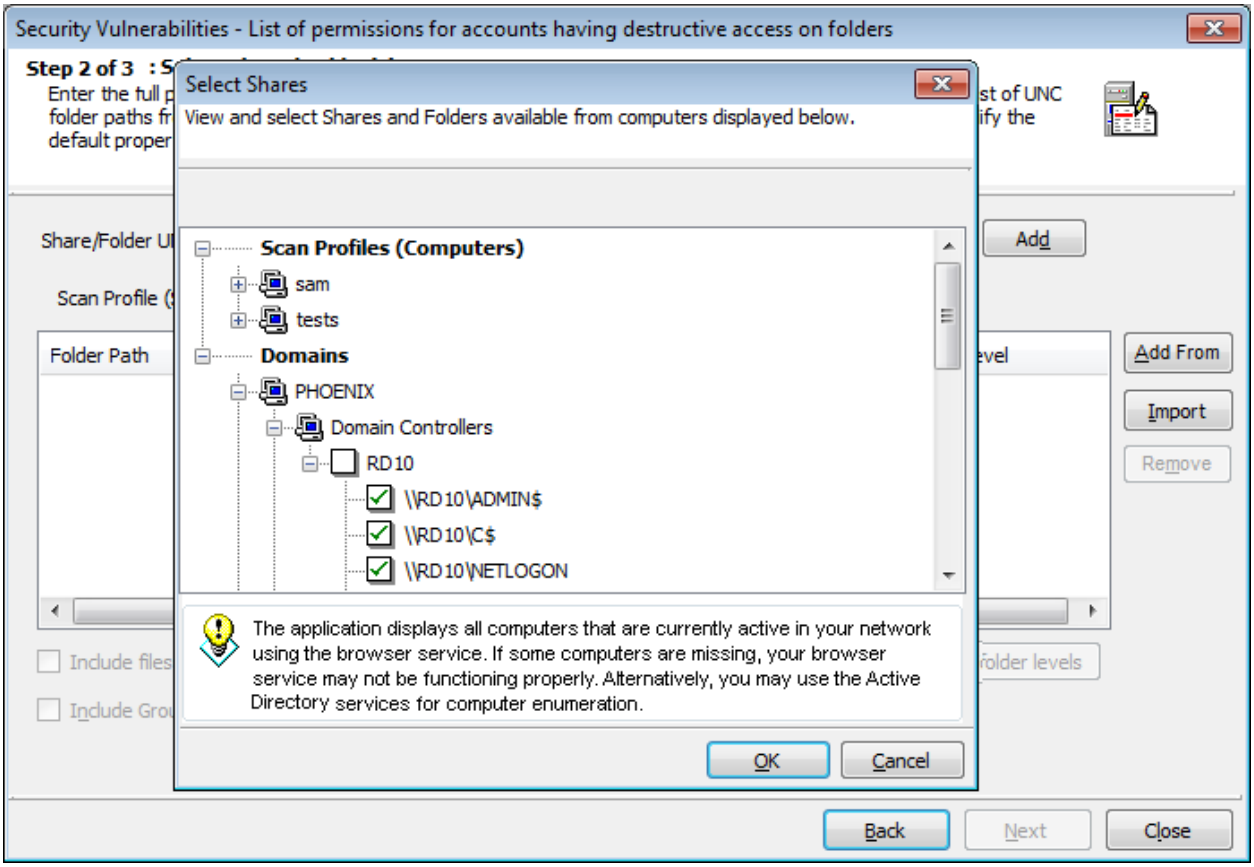
Select the report to be generated. Only one report can be generated at a time.

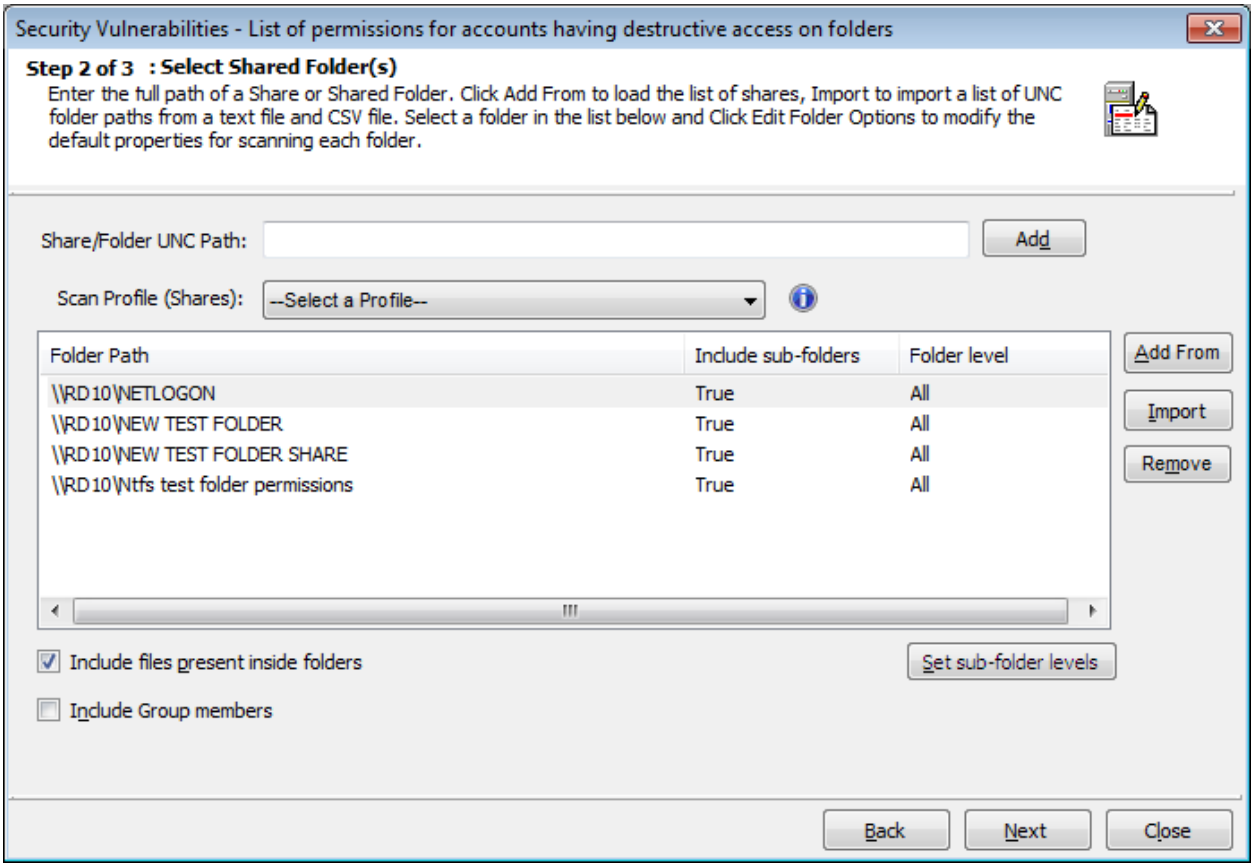

Security Vulnerabilities - List of permissions for accounts having destructive access on folders
Step 1 of 3 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report allows you to view users and groups having destructive access permissions (Full Control, Delete, etc.) on folders
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares.


Security Vulnerabilities - List of permissions for accounts having destructive access on folders
Step 2 of 3
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel
Add
Add From
Import
Remove
Folder Path
Back
Next
Close

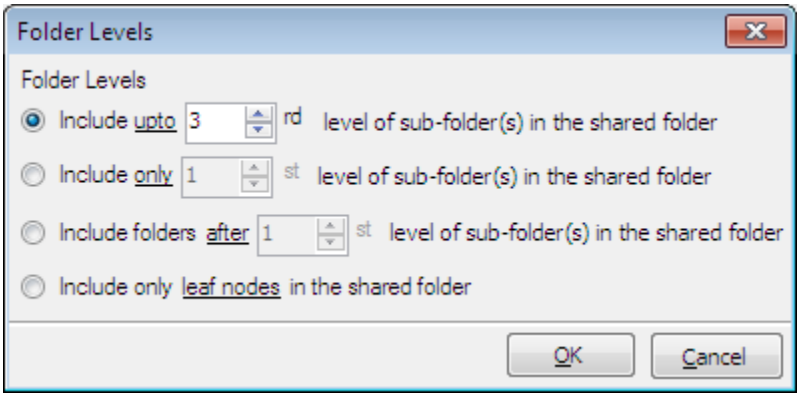

Security Vulnerabilities - List of permissions for accounts having destructive access on folders
Step 2 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Include Group members
Back
Next
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

You can select Include Group members option to include all the members of a group and their sub-group members at all group levels in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

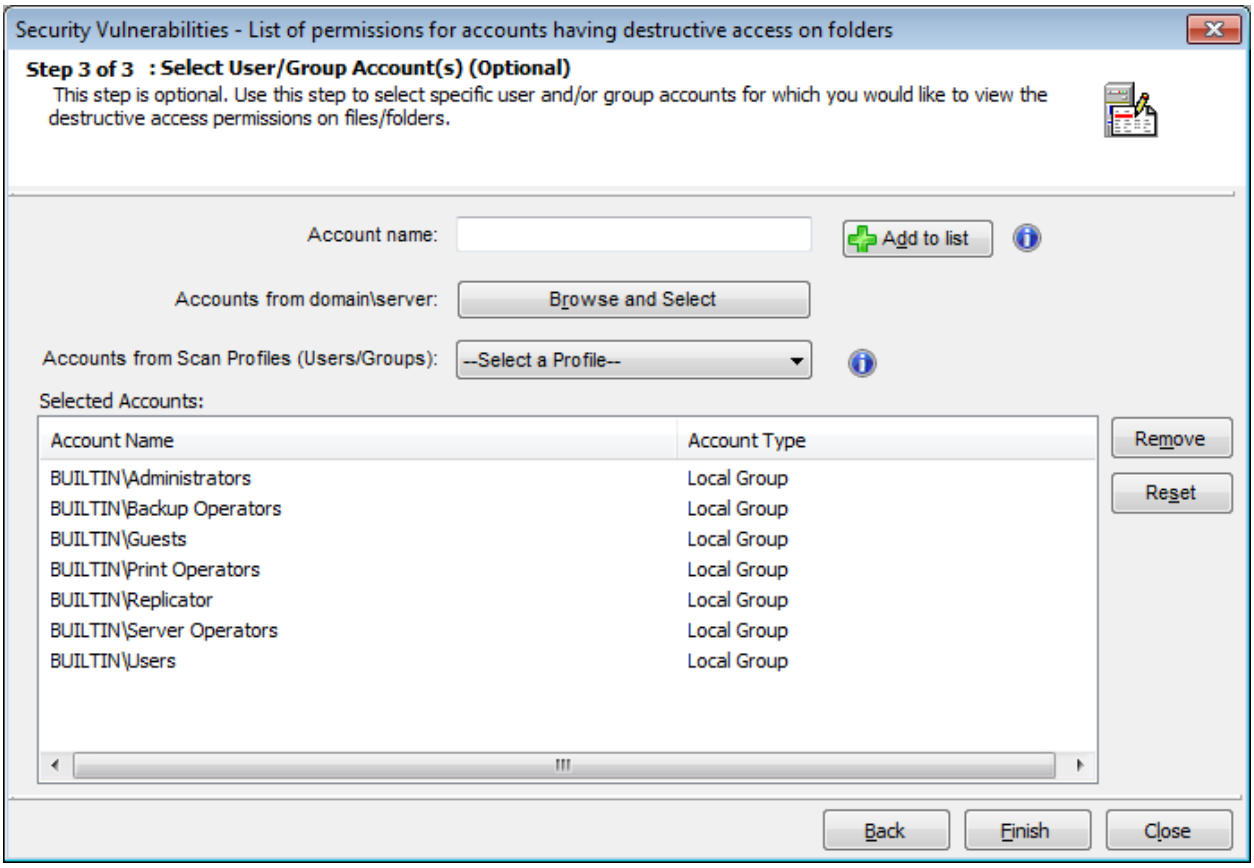
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **Next** to proceed to the next step.

Step 3: Select User/Group Accounts:

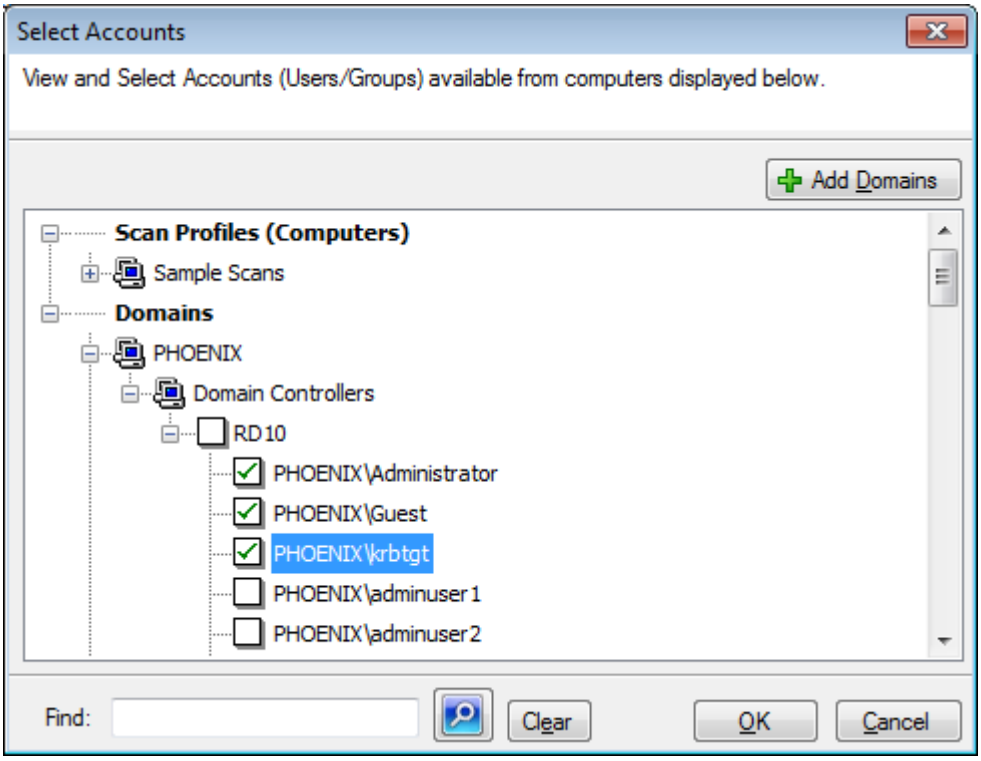
This step is optional. Use this step to select user and/or group accounts for which you like to view the destructive access rights for folders/files.



Enter User/Group name in domain\account name format and click Add to List to add the user/group to the selected accounts list

Use Select a Scan Profile (Users/Groups) option to use the users and groups added in a profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

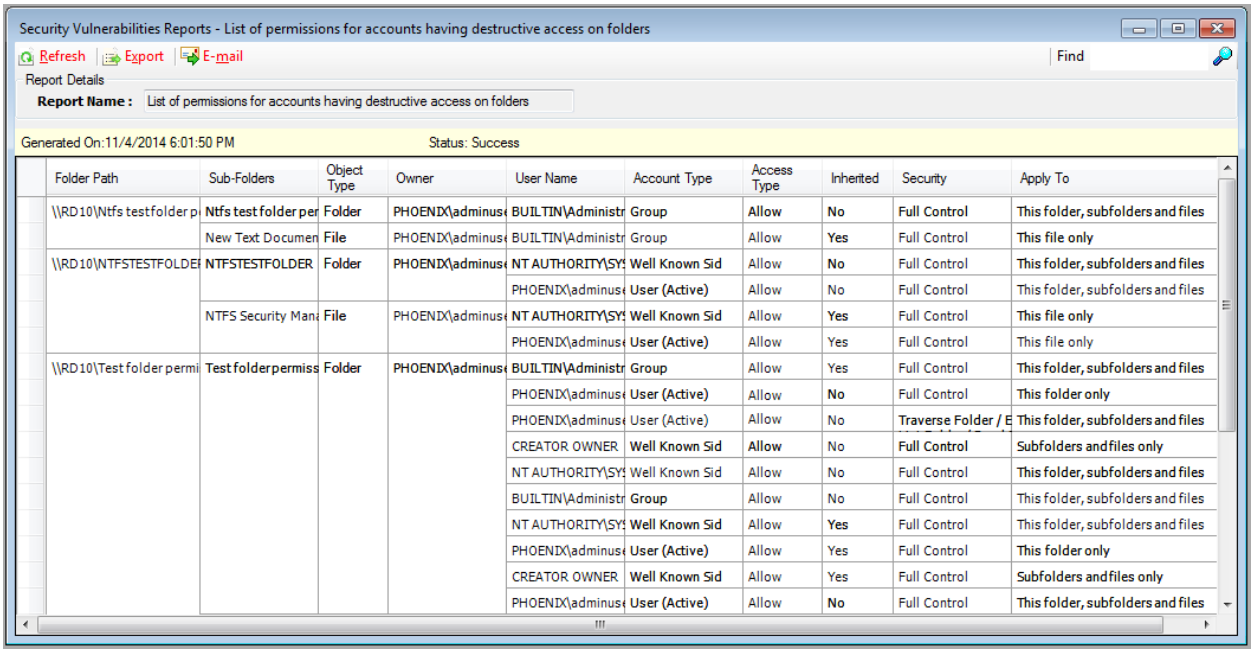
Use Browse and Select option to retrieve users and groups from servers or Scan Profile (Computers).



Use the Find option to search desired user/group accounts.

Click Finish to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:


Security Vulnerabilities Reports - List of permissions for accounts having destructive access on folders
Refresh
Export
E-mail
Find
Report Details
Report Name : List of permissions for accounts having destructive access on folders
Generated On:11/4/2014 6:01:50 PM
Status: Success

Folder Path	Sub-Folders	Object Type	Owner	User Name	Account Type	Access Type	Inherited	Security	Apply To
\\RD10\Ntfs testfolder p	Ntfs testfolder per	Folder	PHOENIX\adminus	BUILTIN\Administr	Group	Allow	No	Full Control	This folder, subfolders and files
	New Text Documen	File	PHOENIX\adminus	BUILTIN\Administr	Group	Allow	Yes	Full Control	This file only
\\RD10\NTFSTESTFOLDE	NTFSTESTFOLDER	Folder	PHOENIX\adminus	NT AUTHORITY\SY	Well Known Sid	Allow	No	Full Control	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	No	Full Control	This folder, subfolders and files
	NTFS Security Mana	File	PHOENIX\adminus	NT AUTHORITY\SY	Well Known Sid	Allow	Yes	Full Control	This file only
				PHOENIX\adminus	User (Active)	Allow	Yes	Full Control	This file only
\\RD10\Test folder permi	Test folder permiss	Folder	PHOENIX\adminus	BUILTIN\Administr	Group	Allow	Yes	Full Control	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	No	Full Control	This folder only
				PHOENIX\adminus	User (Active)	Allow	No	Traverse Folder / E	This folder, subfolders and files
				CREATOR OWNER	Well Known Sid	Allow	No	Full Control	Subfolders and files only
				NT AUTHORITY\SY	Well Known Sid	Allow	No	Full Control	This folder, subfolders and files
				BUILTIN\Administr	Group	Allow	No	Full Control	This folder, subfolders and files
				NT AUTHORITY\SY	Well Known Sid	Allow	Yes	Full Control	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Allow	Yes	Full Control	This folder only
				CREATOR OWNER	Well Known Sid	Allow	Yes	Full Control	Subfolders and files only
				PHOENIX\adminus	User (Active)	Allow	No	Full Control	This folder, subfolders and files

List of folders that have Deny permissions set (both Explicit and Inherited)

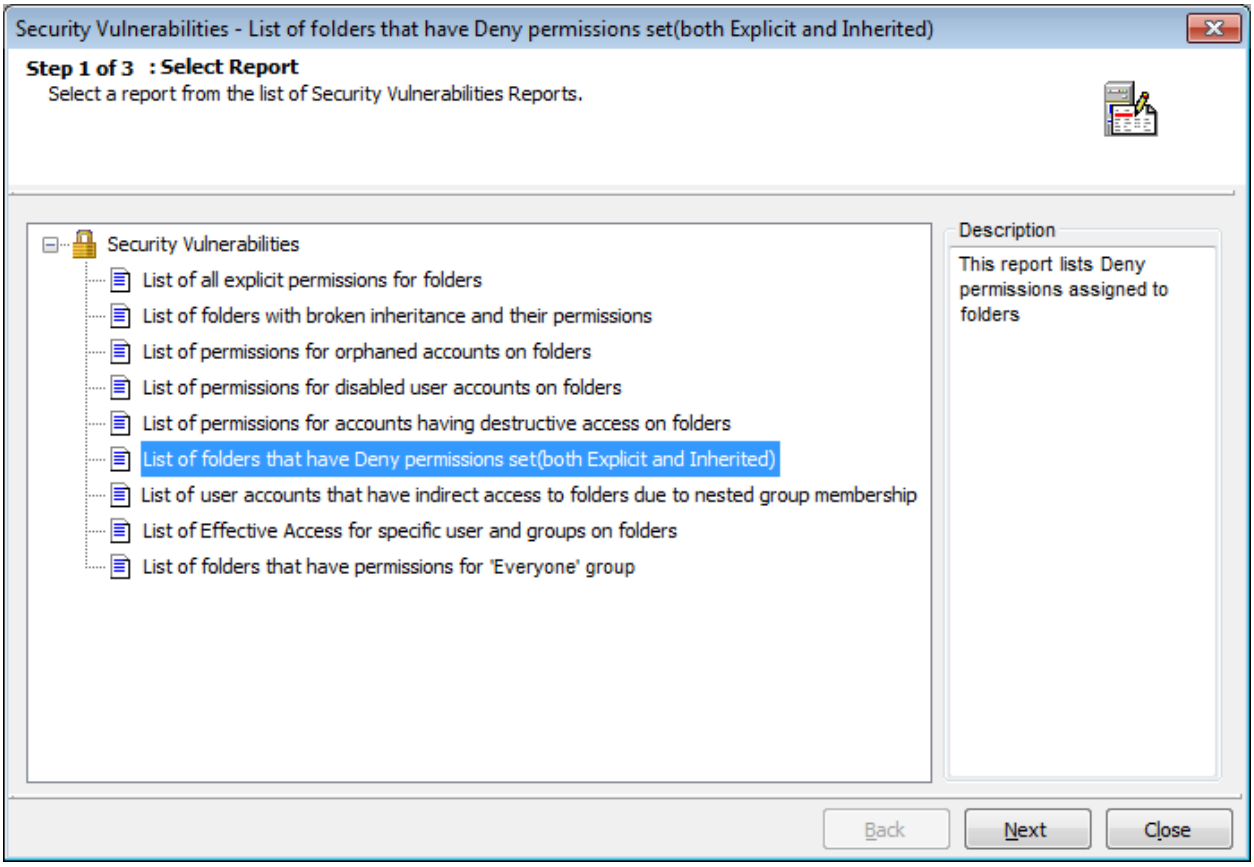
This report allows you to view Deny permissions assigned to folders.

Click on

button.

Step 1: Report Selection

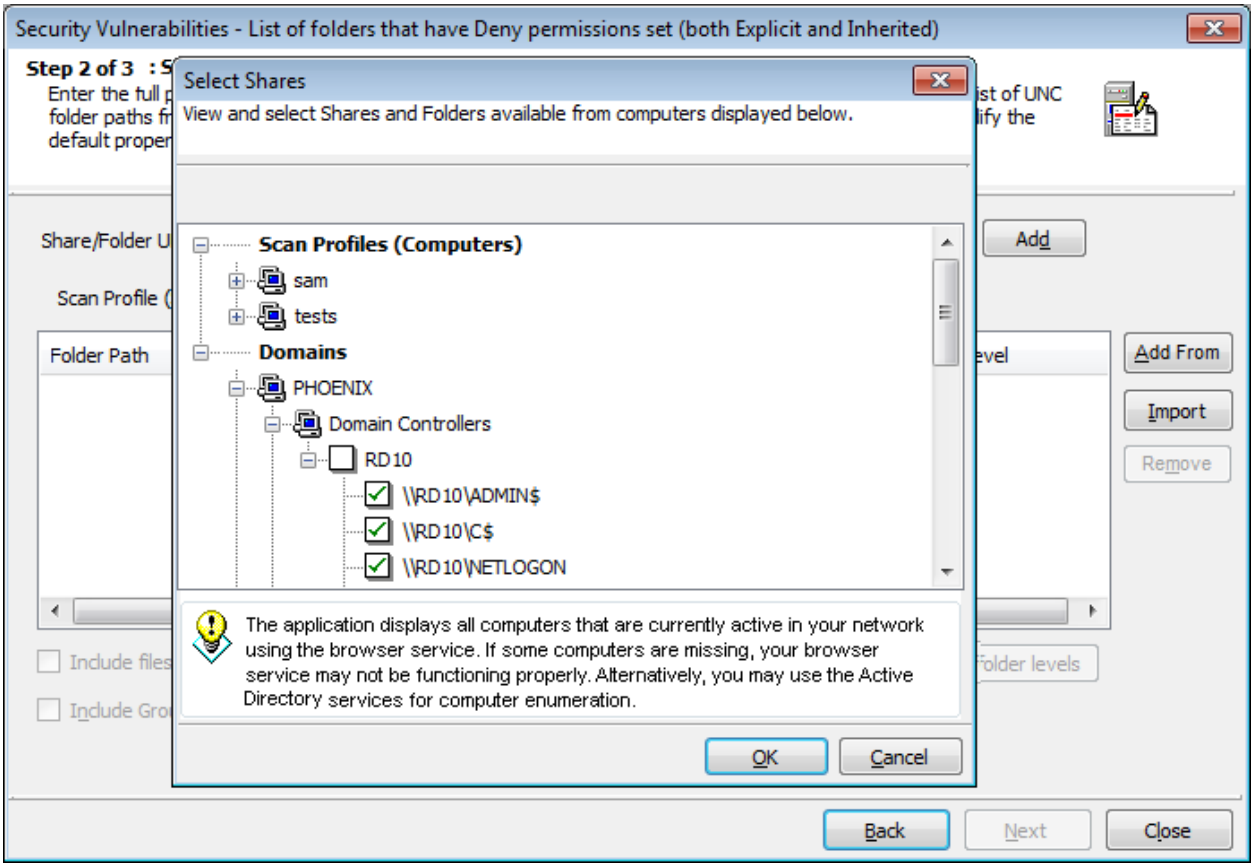
Select the report to be generated. Only one report can be generated at a time.

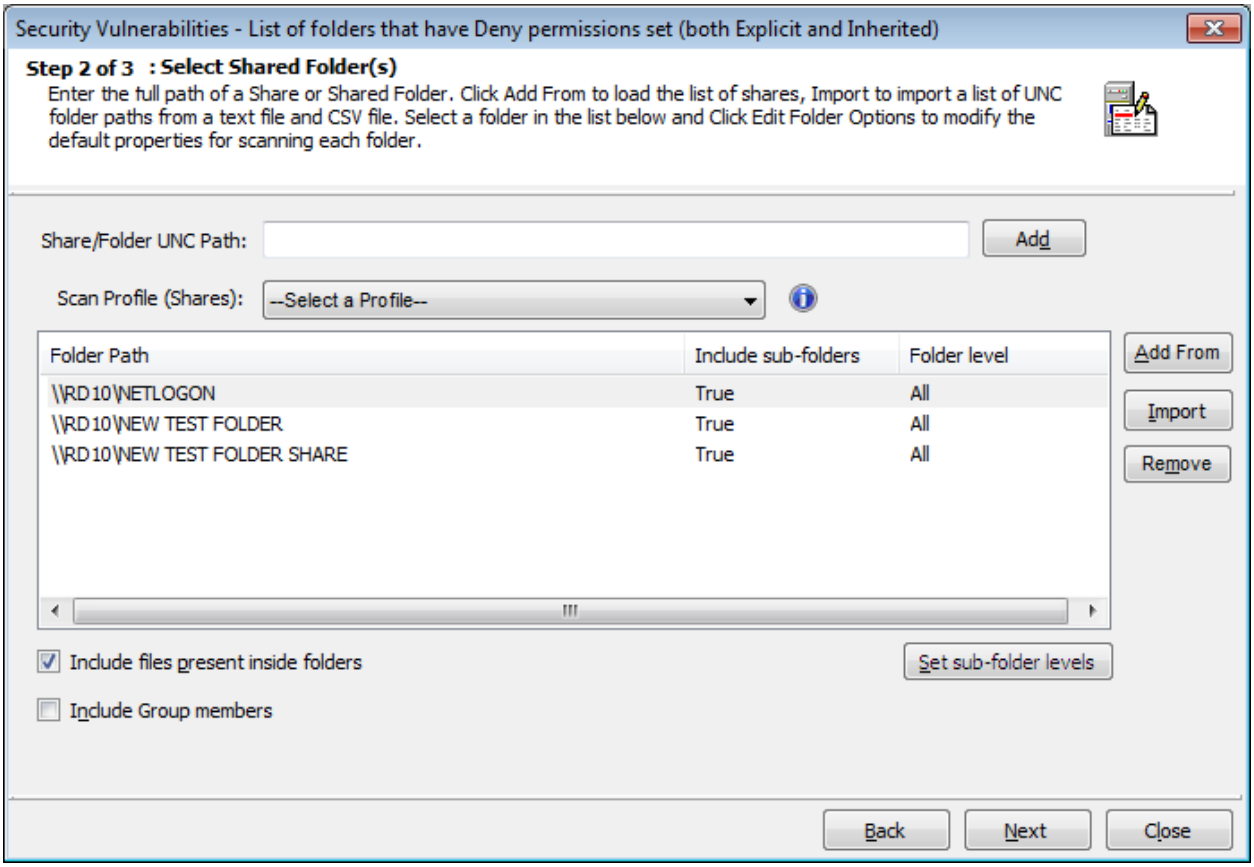

Security Vulnerabilities - List of folders that have Deny permissions set(both Explicit and Inherited)
Step 1 of 3 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists Deny permissions assigned to folders
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select shared folders

Select one or more servers to retrieve available shares.


Security Vulnerabilities - List of folders that have Deny permissions set (both Explicit and Inherited)
Step 2 of 3 : S
Enter the full p
folder paths fr
default proper
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel
Share/Folder U
Scan Profile (
Folder Path
Add
Add From
Import
Remove
Include files
Include Gro
Back
Next
Close

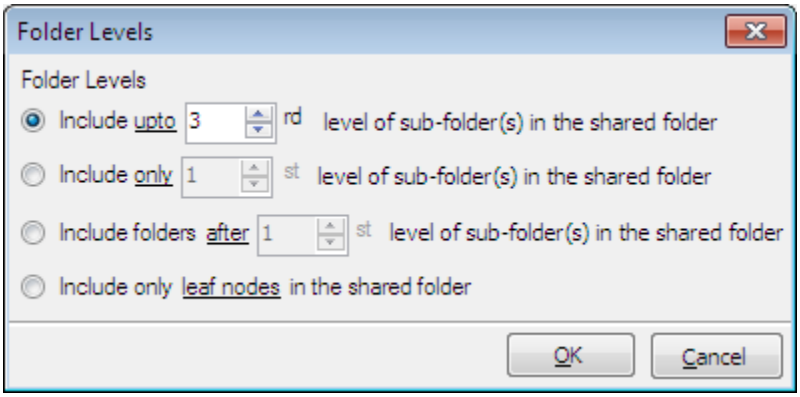

Security Vulnerabilities - List of folders that have Deny permissions set (both Explicit and Inherited)
Step 2 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Include Group members
Back
Next
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

You can select Include Group members option to include all the members of a group and their sub-group members at all group levels in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

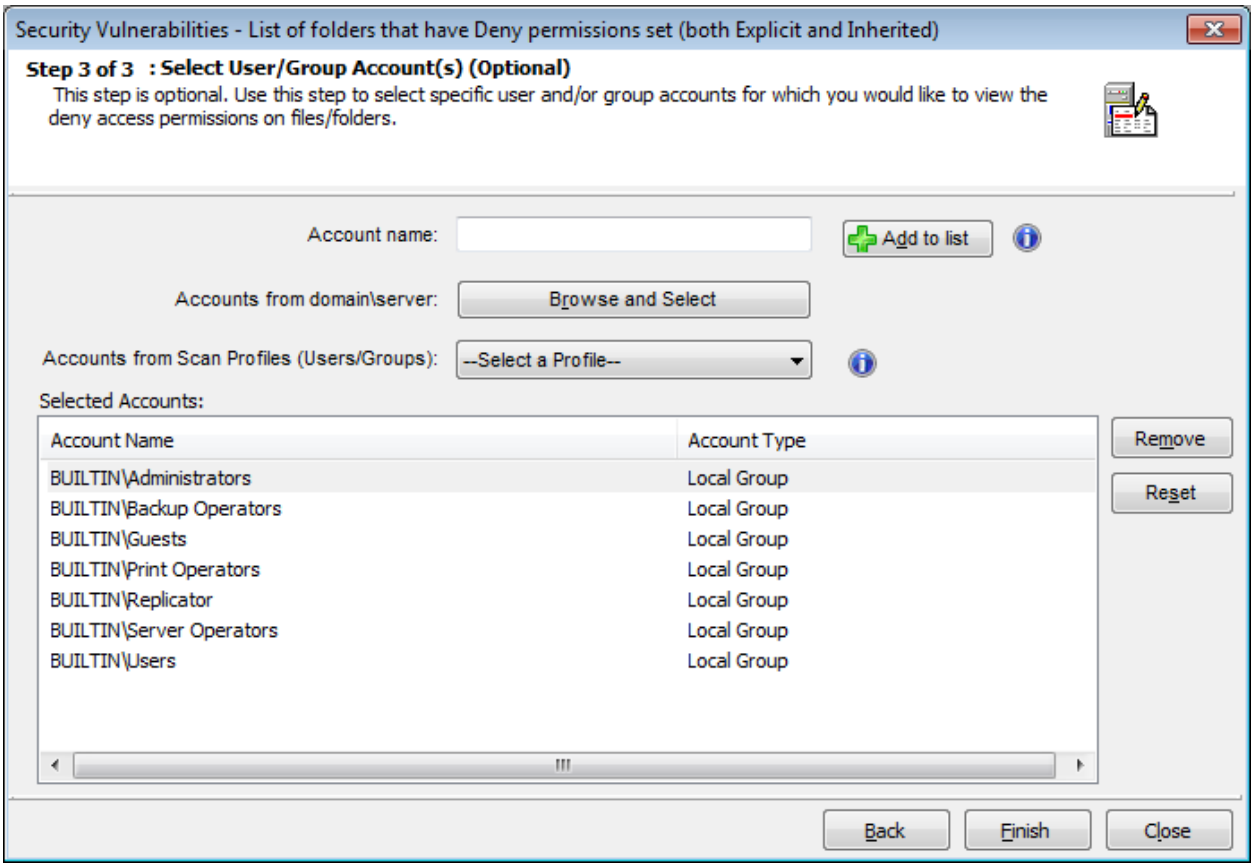
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **Next** to proceed to the next step.

Step 3: Select User/Group Accounts:

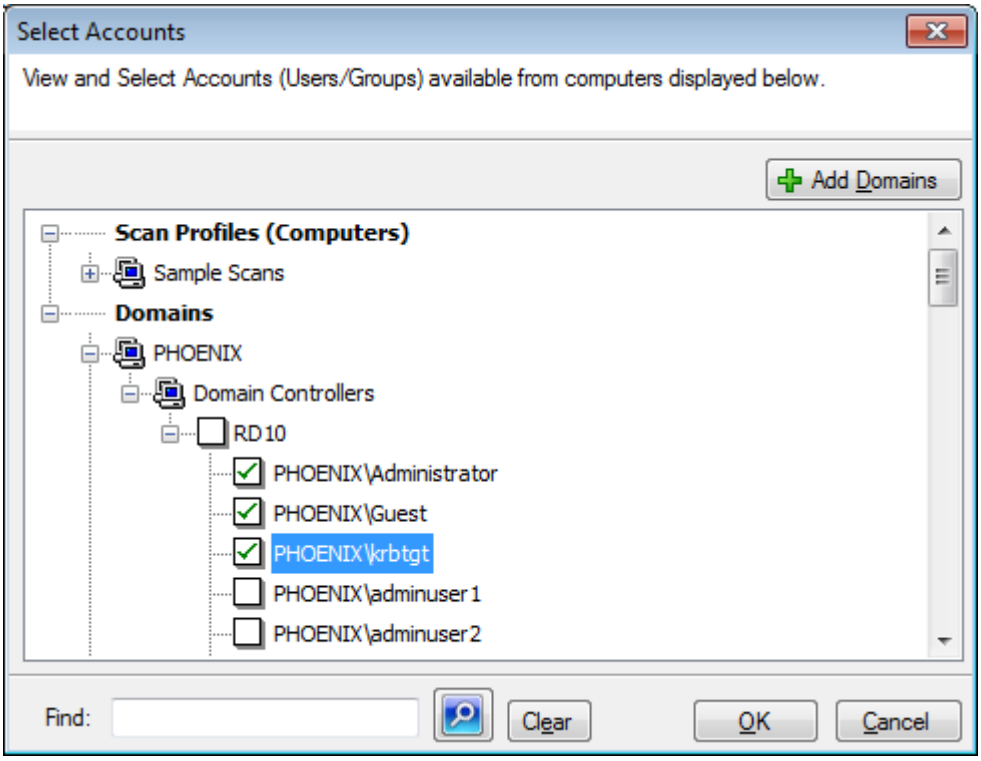
This step is optional. Use this step to select user and/or group accounts for which you like to view the deny permissions for folders/files.



Enter User/Group name in domain\account name format and click Add to List to add the user/group to the selected accounts list

Use Select a Scan Profile (Users/Groups) option to use the users and groups added in a profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

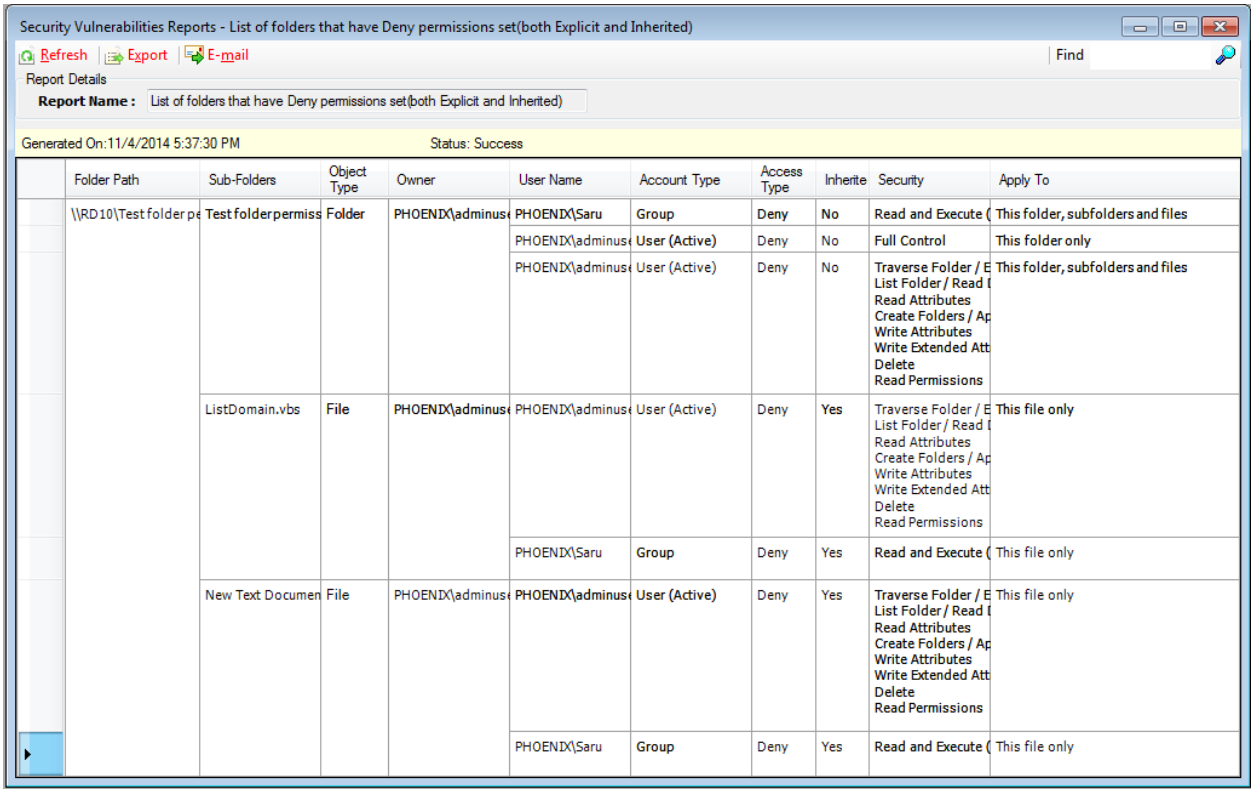
Use Browse and Select option to retrieve users and groups from servers or Scan Profile (Computers).



Use the Find option to search desired user/group accounts.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:


Security Vulnerabilities Reports - List of folders that have Deny permissions set(both Explicit and Inherited)
Refresh
Export
E-mail
Find
Report Details
Report Name : List of folders that have Deny permissions set(both Explicit and Inherited)
Generated On:11/4/2014 5:37:30 PM
Status: Success

Folder Path	Sub-Folders	Object Type	Owner	User Name	Account Type	Access Type	Inherite	Security	Apply To
\\RD10\Test folder pe	Test folder permiss	Folder	PHOENIX\adminus	PHOENIX\Saru	Group	Deny	No	Read and Execute (	This folder, subfolders and files
				PHOENIX\adminus	User (Active)	Deny	No	Full Control	This folder only
				PHOENIX\adminus	User (Active)	Deny	No	Traverse Folder / E List Folder / Read Read Attributes Create Folders / Ap Write Attributes Write Extended Att Delete Read Permissions	This folder, subfolders and files
	ListDomain.vbs	File	PHOENIX\adminus	PHOENIX\adminus	User (Active)	Deny	Yes	Traverse Folder / E List Folder / Read Read Attributes Create Folders / Ap Write Attributes Write Extended Att Delete Read Permissions	This file only
				PHOENIX\Saru	Group	Deny	Yes	Read and Execute (	This file only
	New Text Documen	File	PHOENIX\adminus	PHOENIX\adminus	User (Active)	Deny	Yes	Traverse Folder / E List Folder / Read Read Attributes Create Folders / Ap Write Attributes Write Extended Att Delete Read Permissions	This file only
				PHOENIX\Saru	Group	Deny	Yes	Read and Execute (	This file only

List of user accounts that have indirect access to folders due to nested group membership

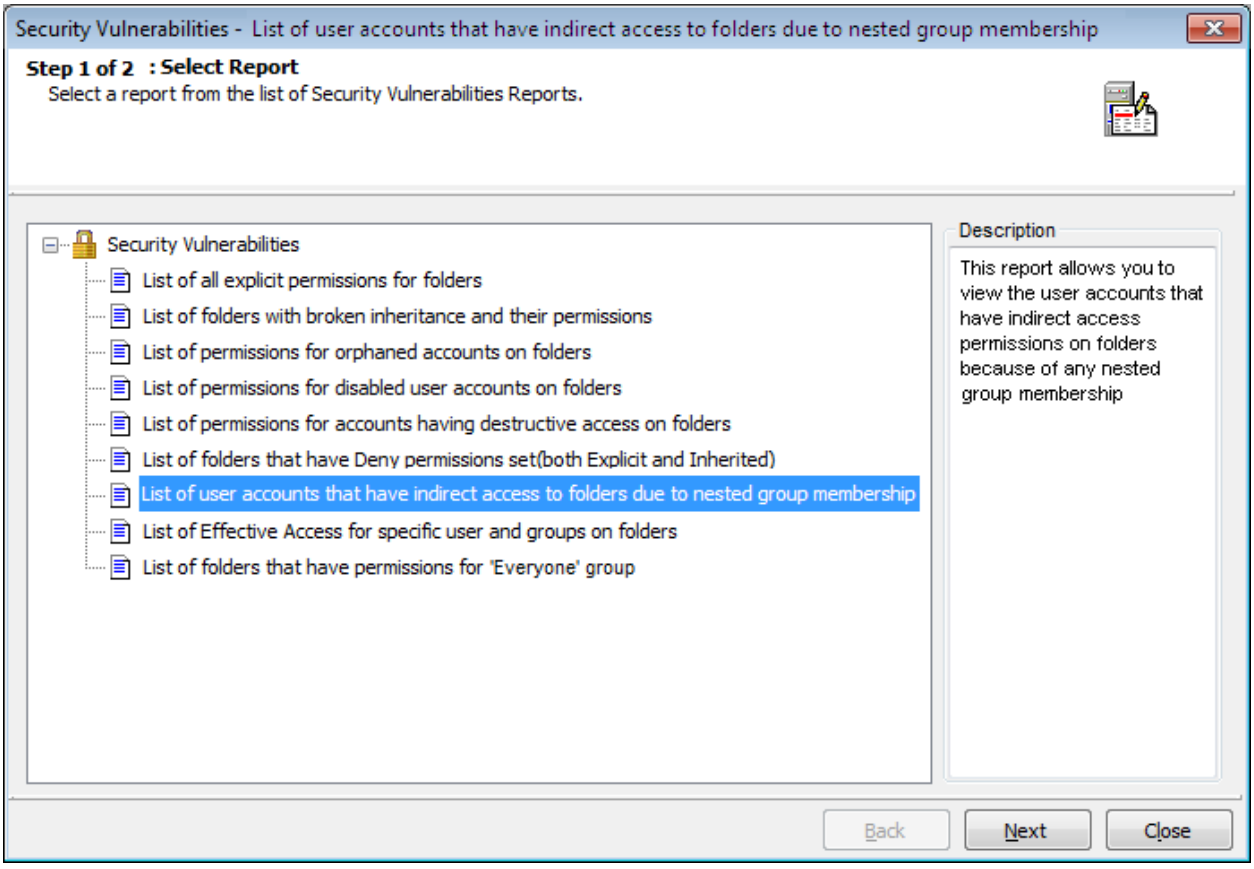
This report allows you to view the user accounts that have indirect access permissions on folders because of any nested group membership.

Click on

button.

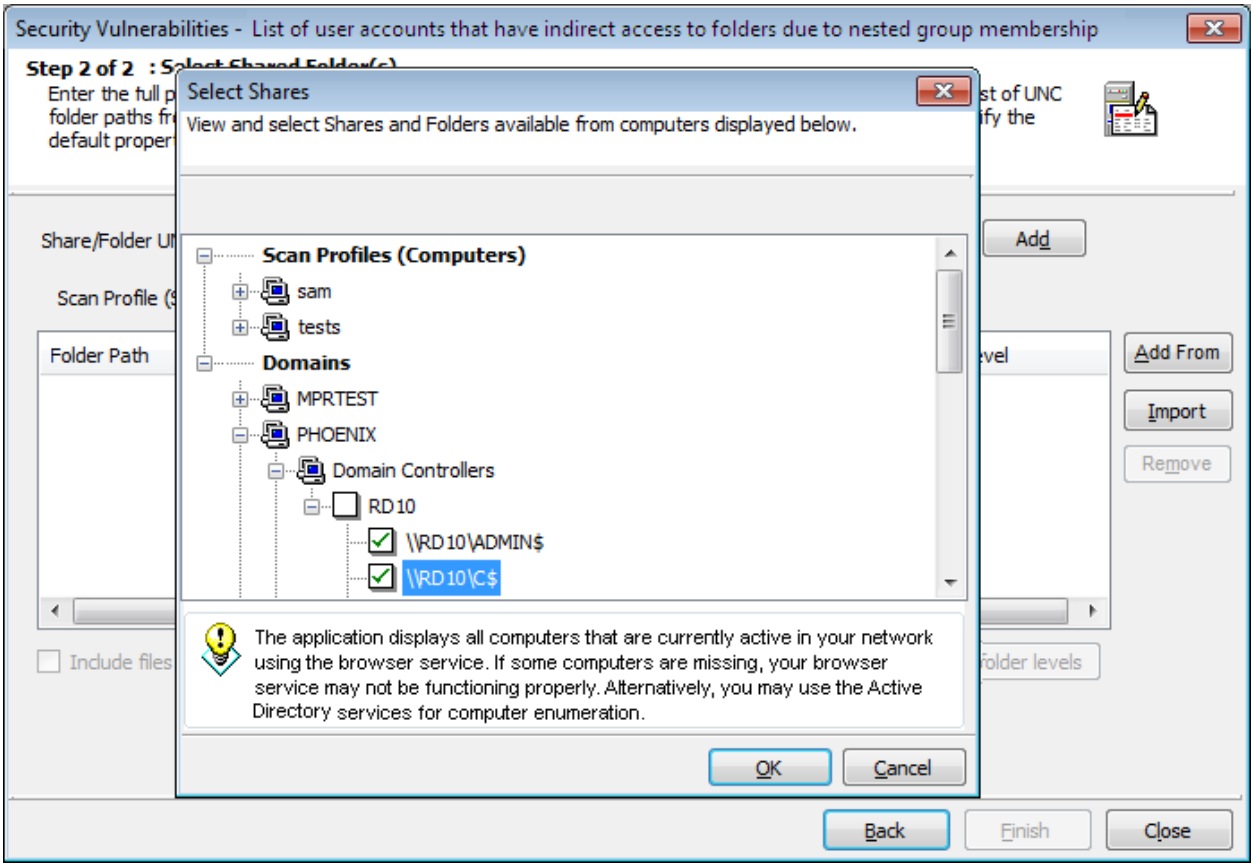
Step 1: Report Selection

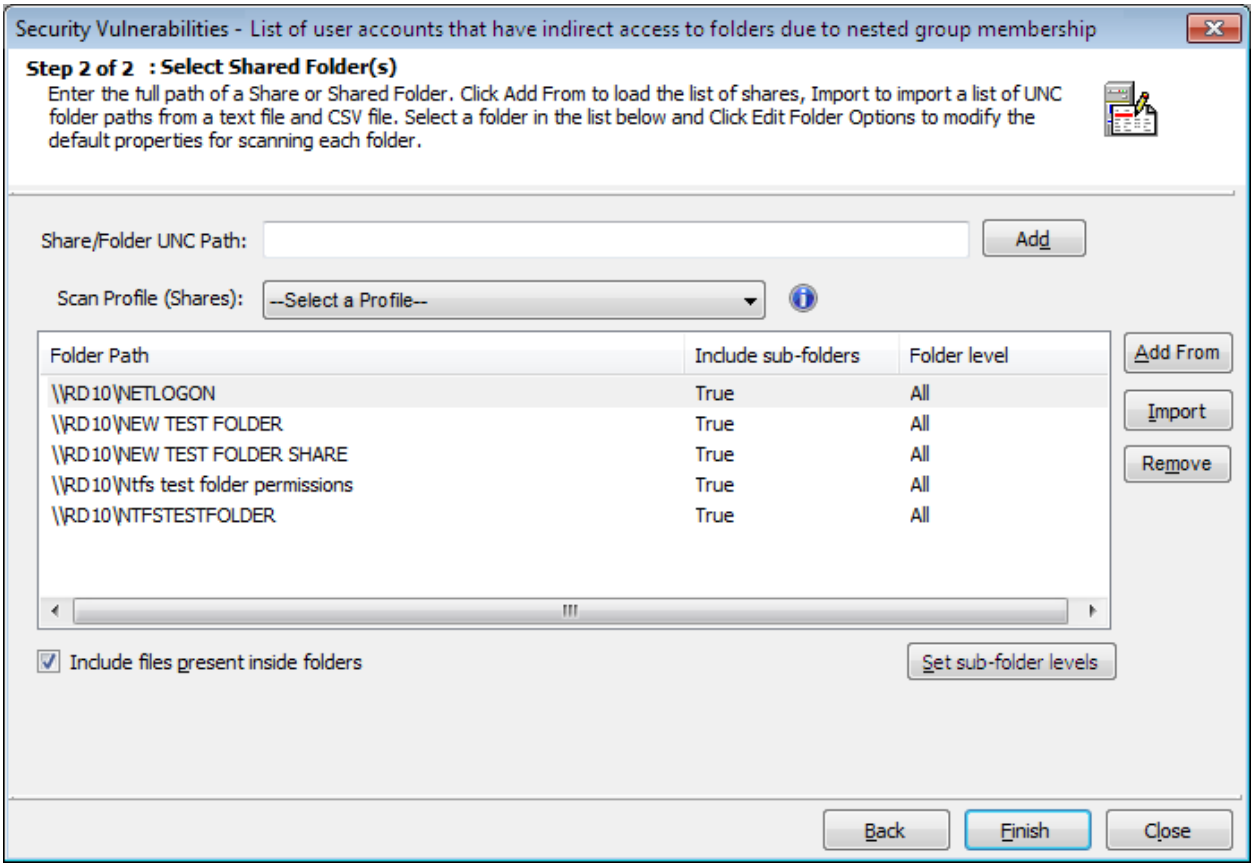
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of user accounts that have indirect access to folders due to nested group membership
Step 1 of 2 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report allows you to view the user accounts that have indirect access permissions on folders because of any nested group membership
Back
Next
Close

Step 2: Select shared folders

Select one or more servers to retrieve available shares.

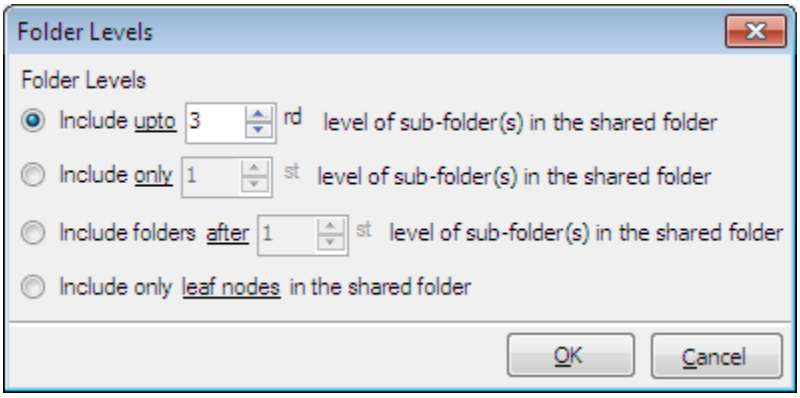

Security Vulnerabilities - List of user accounts that have indirect access to folders due to nested group membership
Step 2 of 2
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel
Add
Add From
Import
Remove
Folder Path
Include files
Back
Finish
Close


Security Vulnerabilities - List of user accounts that have indirect access to folders due to nested group membership
Step 2 of 2 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON
True
All
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
\\RD10\NTFSTESTFOLDER
True
All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Back
Finish
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

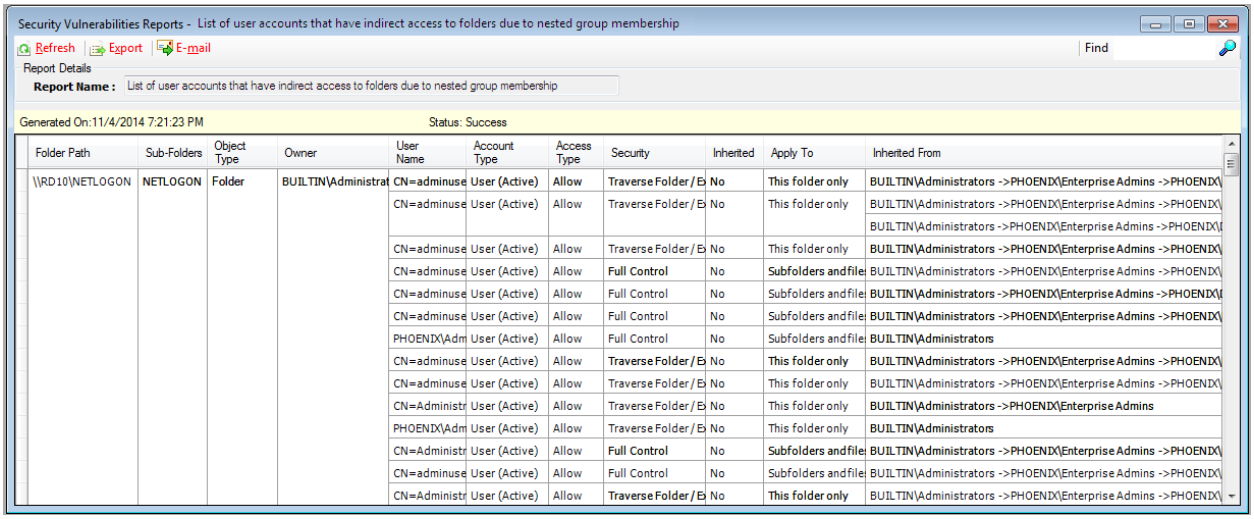
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



List of Effective access for specific users and groups on folders

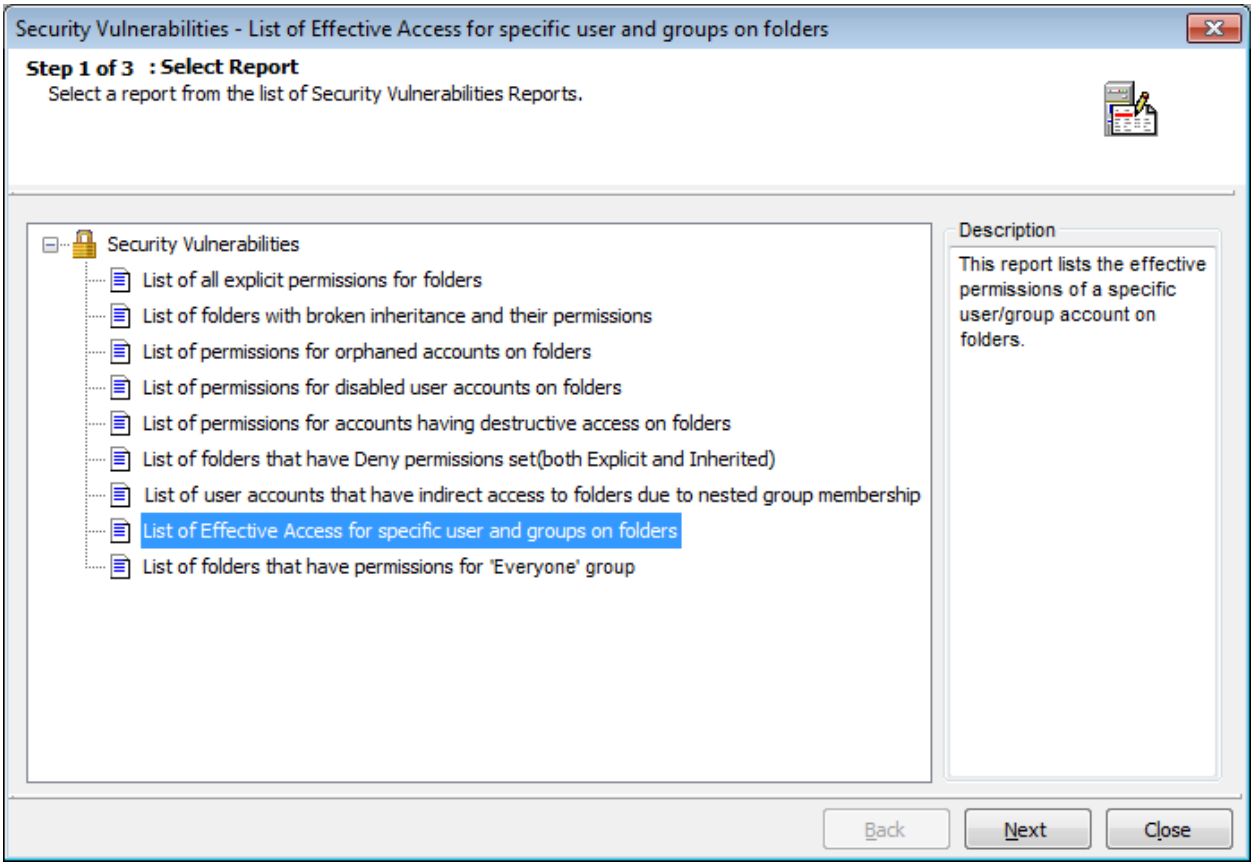
This report allows you to view the effective permissions of specific user/group accounts on folders.

Click on

button.

Step 1: Report Selection

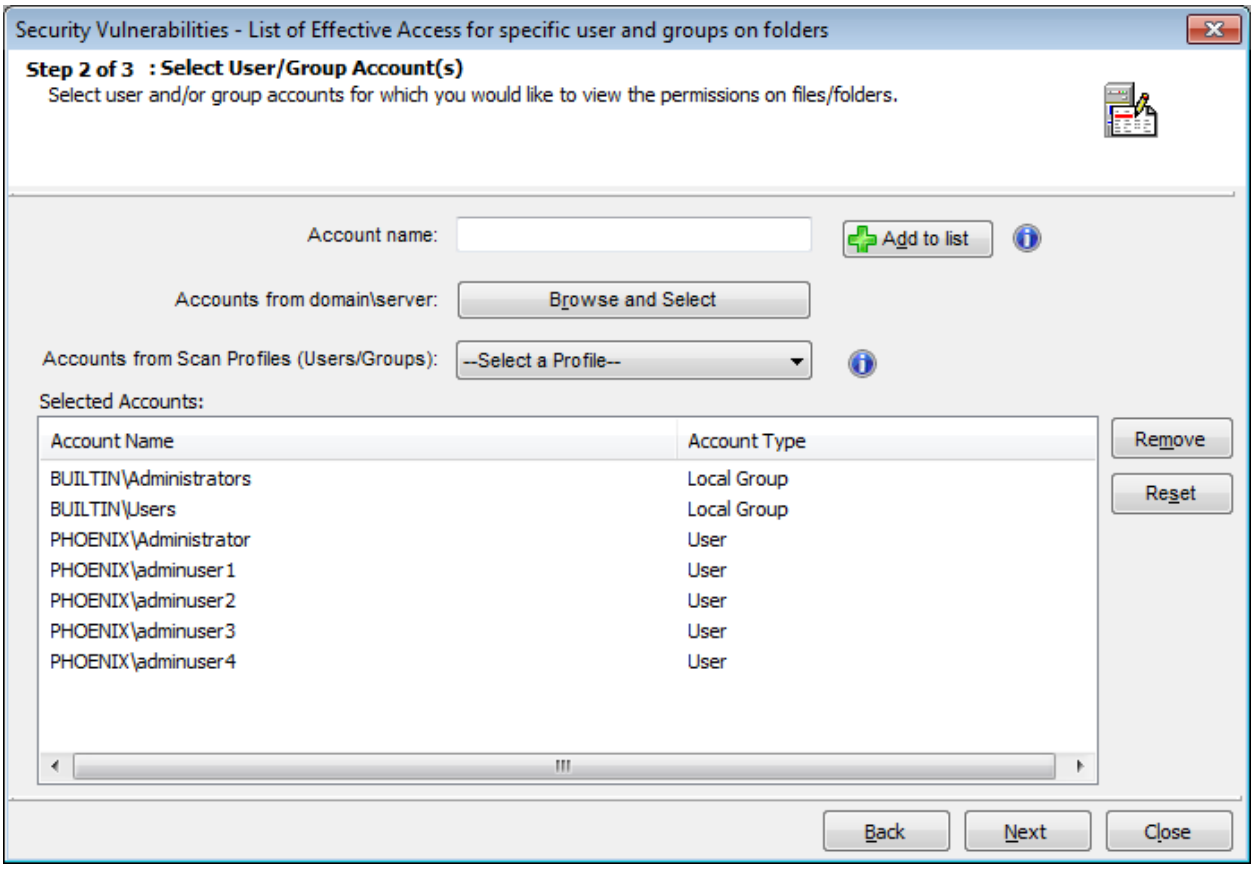
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of Effective Access for specific user and groups on folders
Step 1 of 3 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists the effective permissions of a specific user/group account on folders.
Back
Next
Close

Click **Next** to proceed to the next step.

Step 2: Select User/Group Accounts:

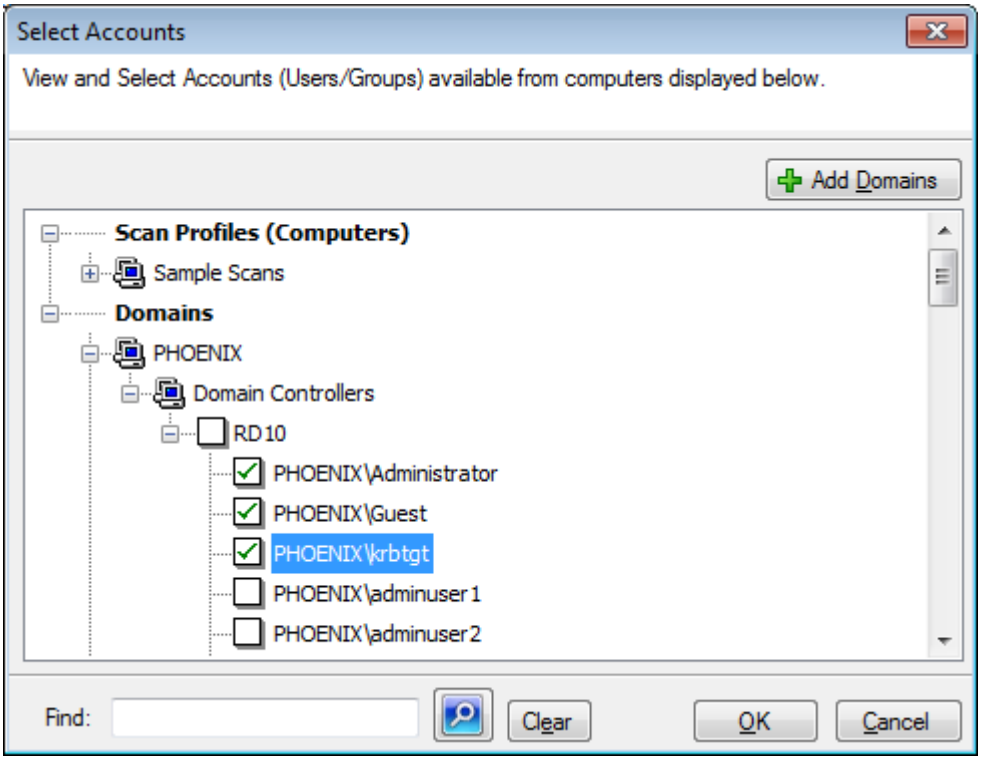
Select user and/or group accounts for which you like to view the effective permissions for folders/files.



Enter User/Group name in domain\account name format and click Add to List to add the user/group to the selected accounts list

Use Select a Scan Profile (Users/Groups) option to use the users and groups added in a profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

Use Browse and Select option to retrieve users and groups from servers or Scan Profile (Computers).

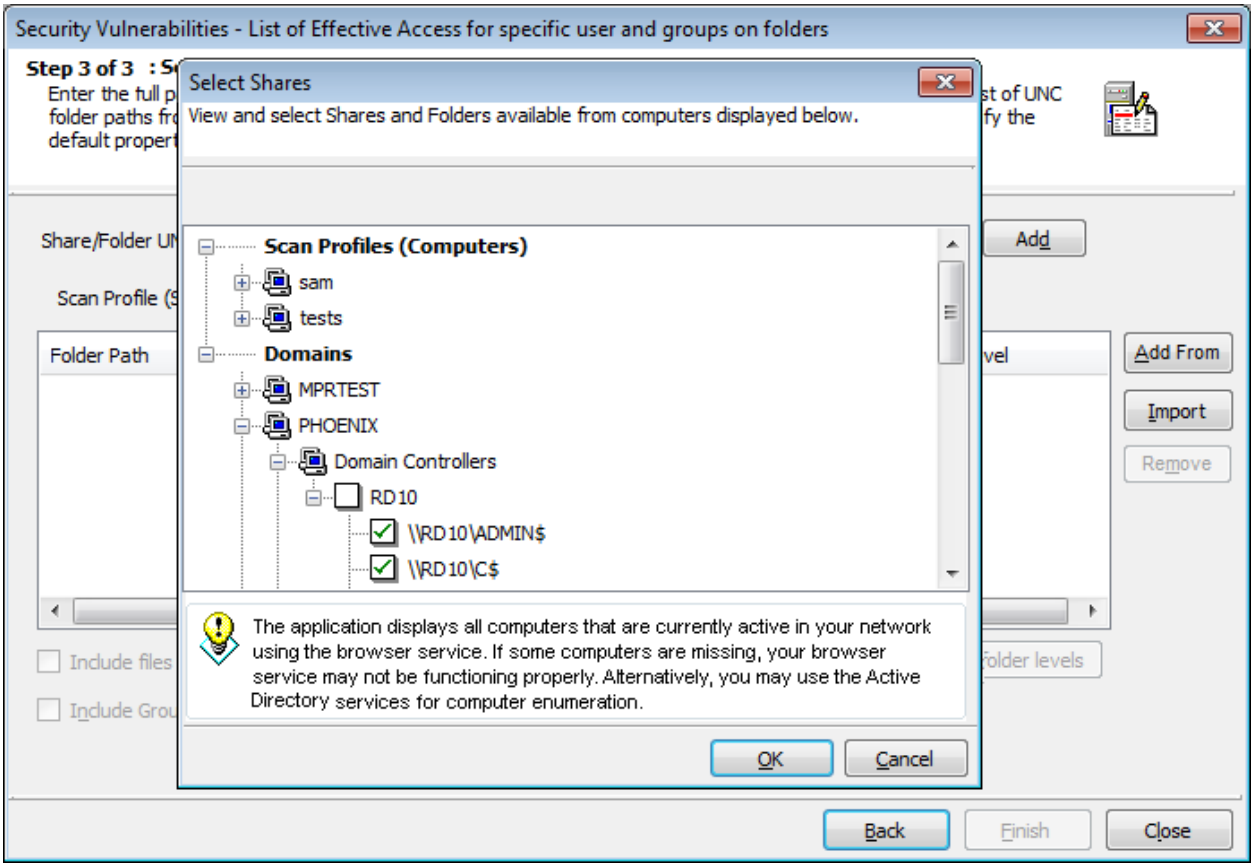


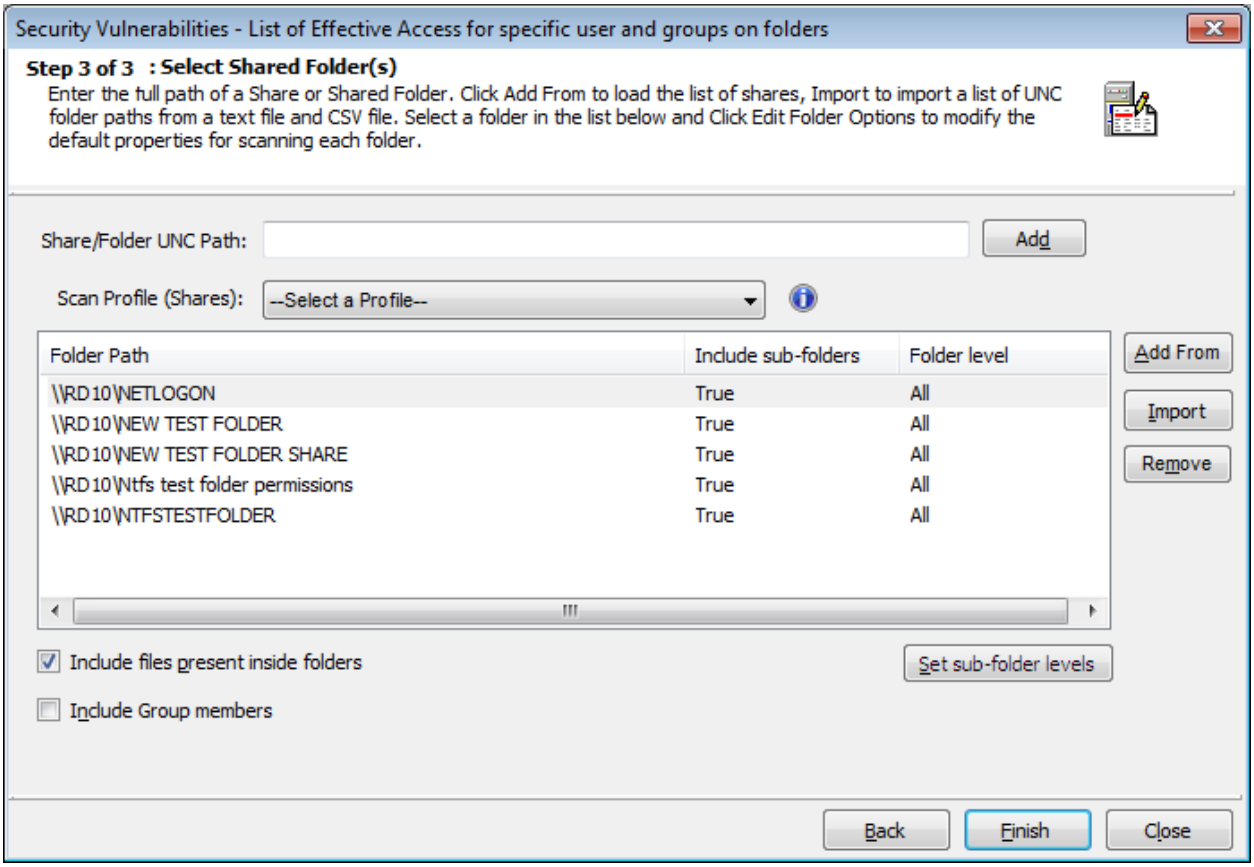
Use the Find option to search desired user/group accounts.

Click **Next** to proceed.

Step 3: Select shared folders

Select one or more servers to retrieve available shares.


Security Vulnerabilities - List of Effective Access for specific user and groups on folders
Step 3 of 3
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel
Add
Add From
Import
Remove
Folder Path
Include files
Back
Finish
Close

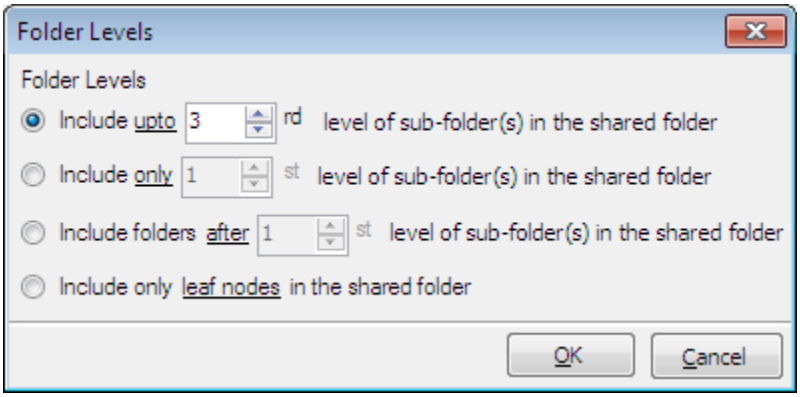

Security Vulnerabilities - List of Effective Access for specific user and groups on folders
Step 3 of 3 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON True All
\\RD10\NEW TEST FOLDER True All
\\RD10\NEW TEST FOLDER SHARE True All
\\RD10\Ntfs test folder permissions True All
\\RD10\NTFSTESTFOLDER True All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Include Group members
Back
Finish
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

You can select Include Group members option to include all the members of a group and their sub-group members at all group levels in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

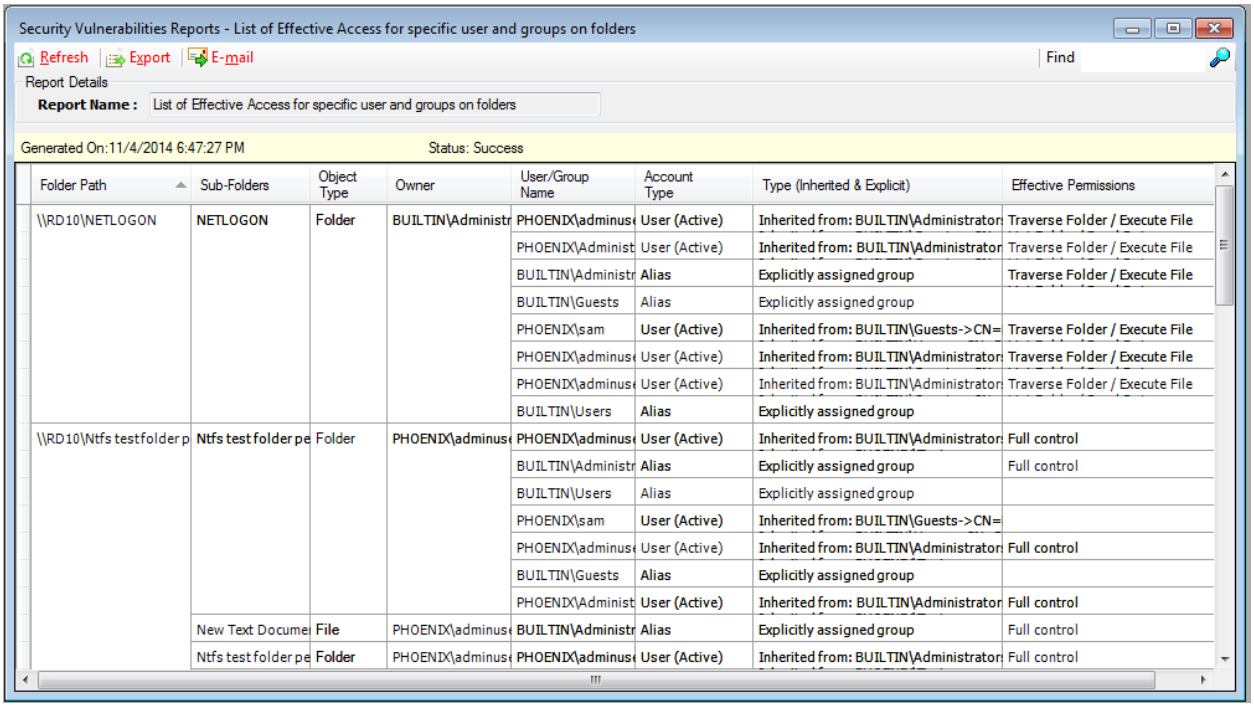
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



List of folders that have permissions for 'Everyone' group

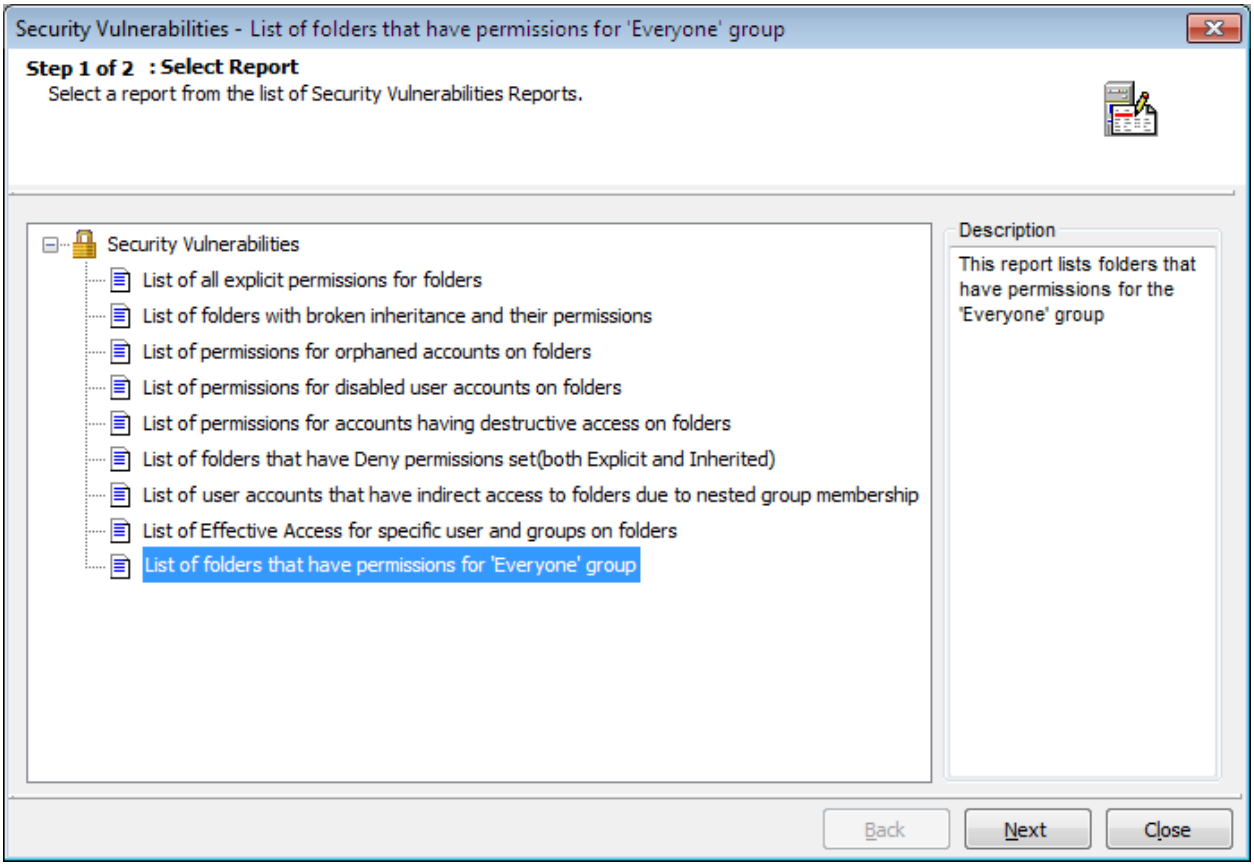
This report allows you to view the folders that have permissions for 'Everyone' group.

Click on

button.

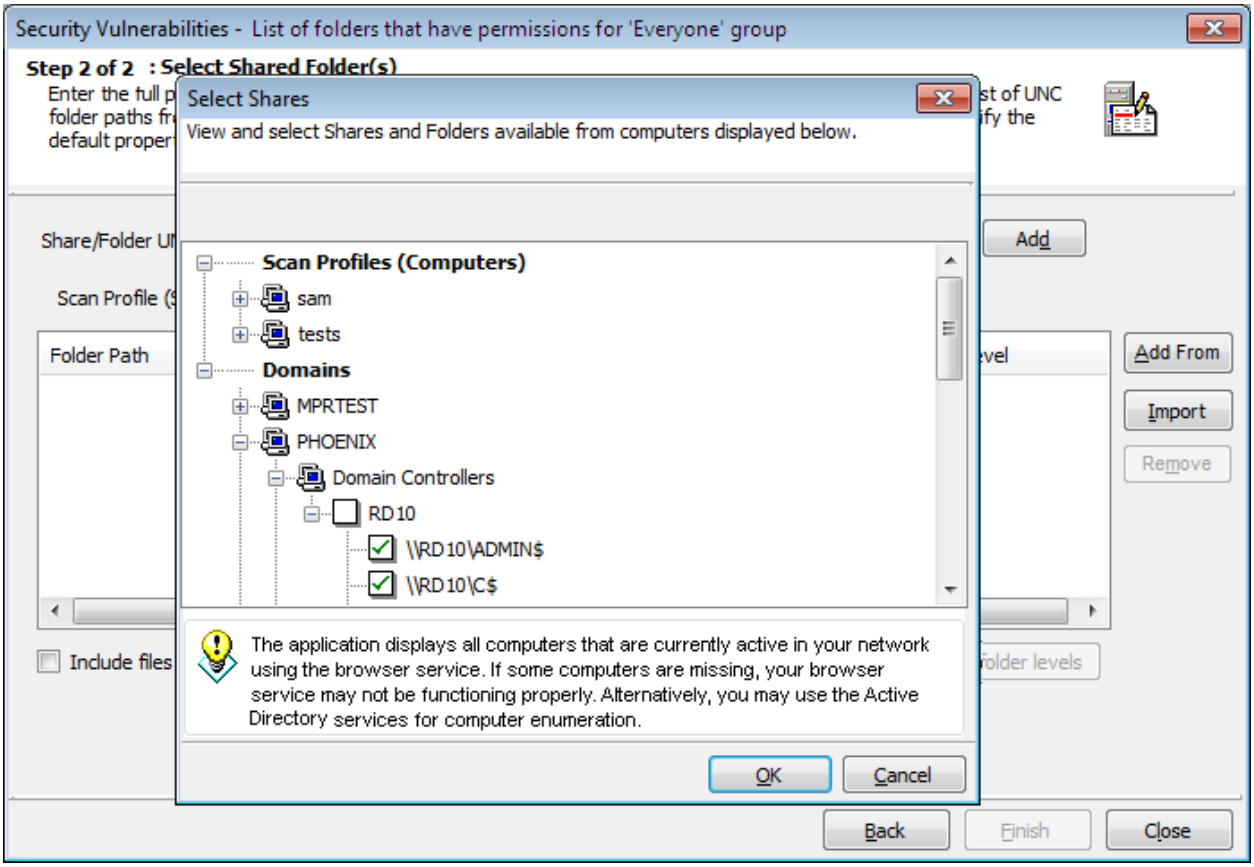
Step 1: Report Selection

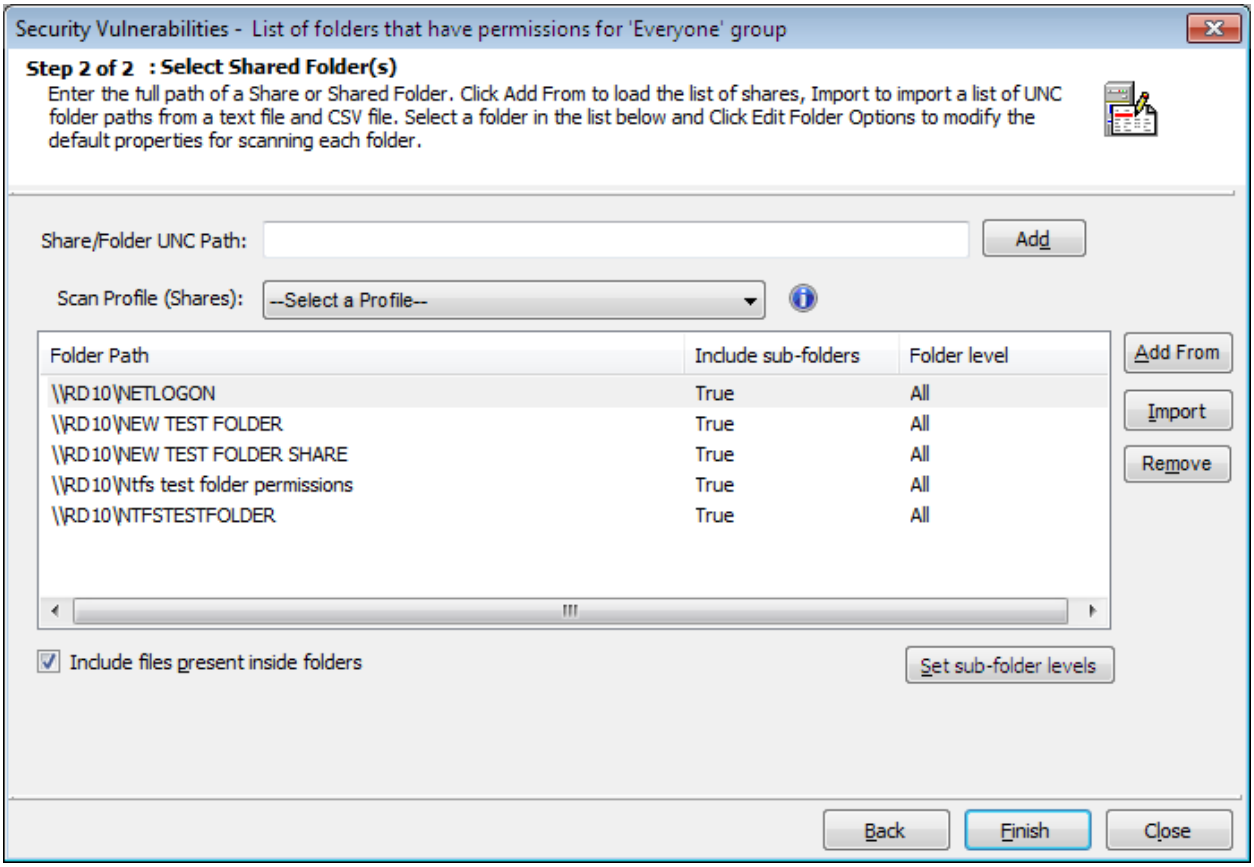
Select the report to be generated. Only one report can be generated at a time.


Security Vulnerabilities - List of folders that have permissions for 'Everyone' group
Step 1 of 2 : Select Report
Select a report from the list of Security Vulnerabilities Reports.
Security Vulnerabilities
List of all explicit permissions for folders
List of folders with broken inheritance and their permissions
List of permissions for orphaned accounts on folders
List of permissions for disabled user accounts on folders
List of permissions for accounts having destructive access on folders
List of folders that have Deny permissions set(both Explicit and Inherited)
List of user accounts that have indirect access to folders due to nested group membership
List of Effective Access for specific user and groups on folders
List of folders that have permissions for 'Everyone' group
Description
This report lists folders that have permissions for the 'Everyone' group
Back
Next
Close

Step 2: Select shared folders

Select one or more servers to retrieve available shares.

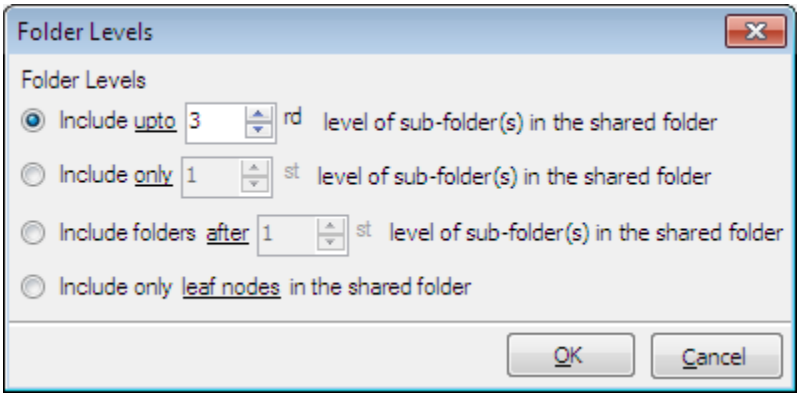

Security Vulnerabilities - List of folders that have permissions for 'Everyone' group
Step 2 of 2 : Select Shared Folder(s)
Enter the full p
folder paths fr
default proper
st of UNC
ify the
Share/Folder UI
Add
Scan Profile (S
Folder Path
Add From
Import
Remove
Include files
older levels
Back
Finish
Close
Select Shares
View and select Shares and Folders available from computers displayed below.
Scan Profiles (Computers)
sam
tests
Domains
MPRTEST
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
The application displays all computers that are currently active in your network using the browser service. If some computers are missing, your browser service may not be functioning properly. Alternatively, you may use the Active Directory services for computer enumeration.
OK
Cancel


Security Vulnerabilities - List of folders that have permissions for 'Everyone' group
Step 2 of 2 : Select Shared Folder(s)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NETLOGON True All
\\RD10\NEW TEST FOLDER True All
\\RD10\NEW TEST FOLDER SHARE True All
\\RD10\Ntfs test folder permissions True All
\\RD10\NTFSTESTFOLDER True All
Add From
Import
Remove
Include files present inside folders
Set sub-folder levels
Back
Finish
Close

You may also enter the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

You can select Include files present inside folders option to include all files from the specified folders in the report.

Use Set sub-folder levels option to view permissions in the selected levels of sub-folder(s) in the shared folder.


Folder Levels
Folder Levels
Include upto 3 rd level of sub-folder(s) in the shared folder
Include only 1 st level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are in the specified folder level only.

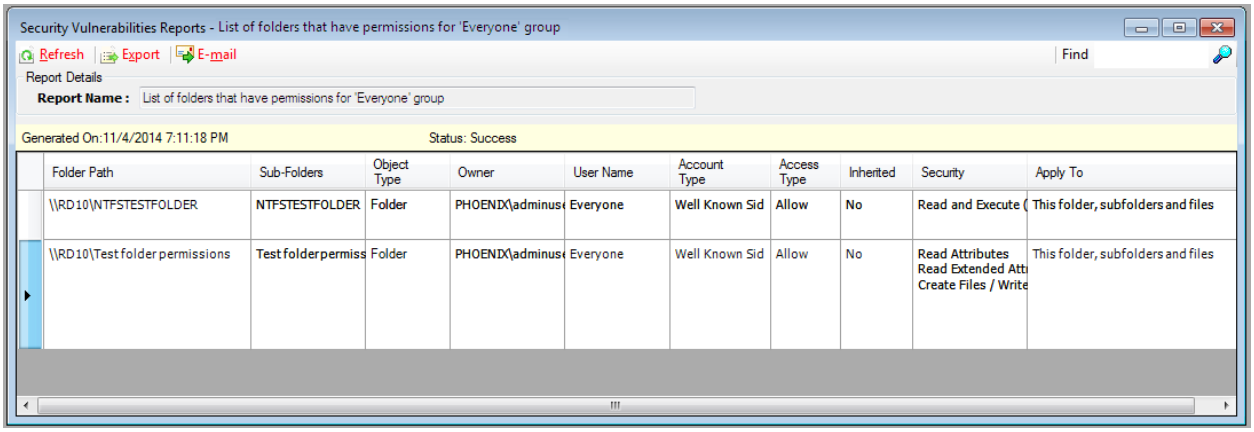
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will view permissions from sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will view permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **OK** to proceed.

Click **Finish** to generate the selected report.

Once the data collection process is complete, the report would be generated in a report window as shown below:



Power Export

About Power Export

Task Manager

Schedule Standard Reports

Schedule Built-in Reports

About Power Export

NTFS Security Auditor provides a powerful offline report generation tool called Power Export. Power Export allows the user to select multiple reports to be run for several domains and servers across the enterprise at scheduled intervals. The Power Export tool has the ability to export and/or email the reports in different file formats.

Please note the following while using the Power Export Wizard:

a. Scheduled reports will be created as a "task" in Windows Task Scheduler.
b. The scheduled job will generate and export/email the reports in different file formats (HTML, CSV , XLSX and SQL) to the desired folder path/printer.
c. By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected Reports will be exported to a time-stamped sub-folder, in the format "yyyy-mm-dd hh.mm.ss", under the task name folder. Therefore, the full folder path for all the exported reports refers to the following directory: <Export path><Task name><Time stamp>.
d. A separate file will be created for each report in the desired file format. For example, in the HTML file format, each report will be created as a.html file.

Note: NTFS Security Auditor Power Export Wizard will help you create and store the settings for a task, which you may view or modify later using the Scheduled Tasks Manager. The task will be created with the settings (Schedule Type and Run As parameter) provided using the Power Export Wizard. A valid password must be specified for the Run As parameter of the task.

You can schedule the two types of reports (Shares, Folder and Files report and Built-in report) available in NTFS Security Auditor.

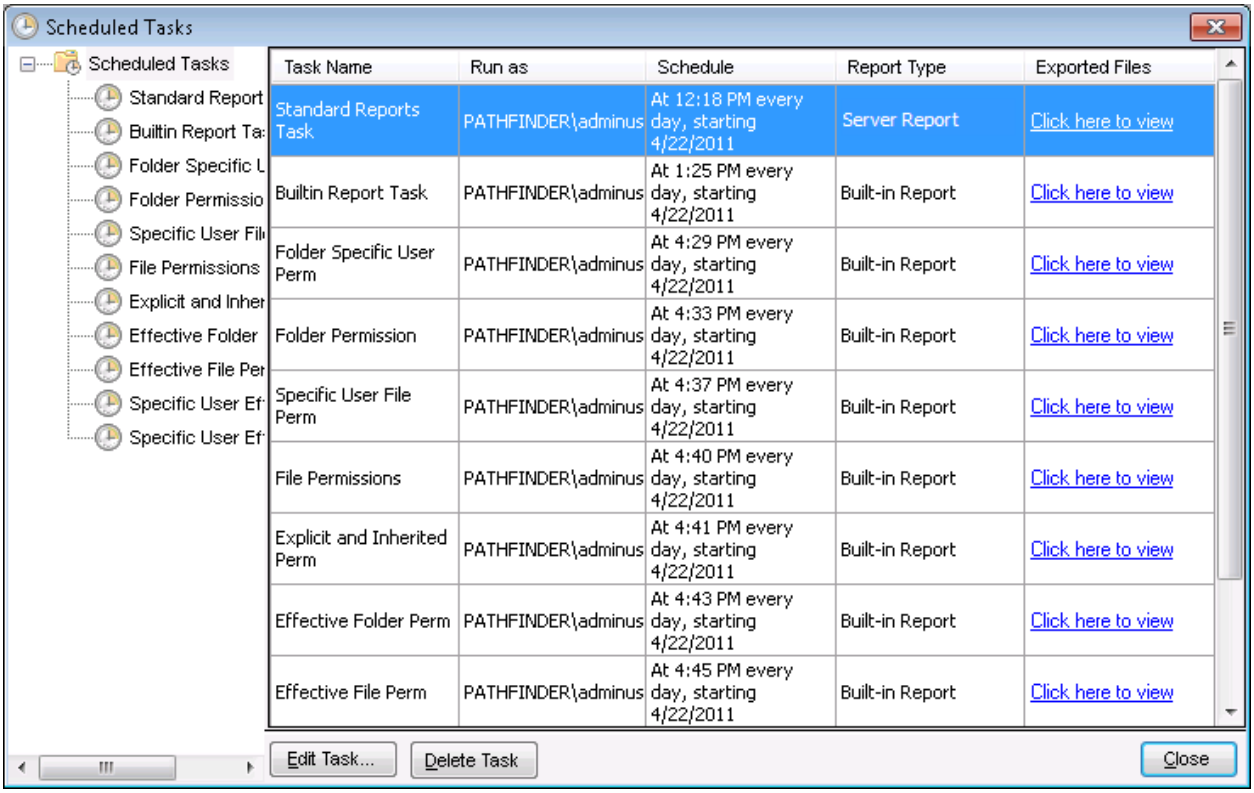
Scheduled Tasks Manager

The Scheduled Tasks Manager allows you to perform the following operations:

- View summary information for the tasks created
- View exported files of the task
- Edit an existing task
- Delete a task

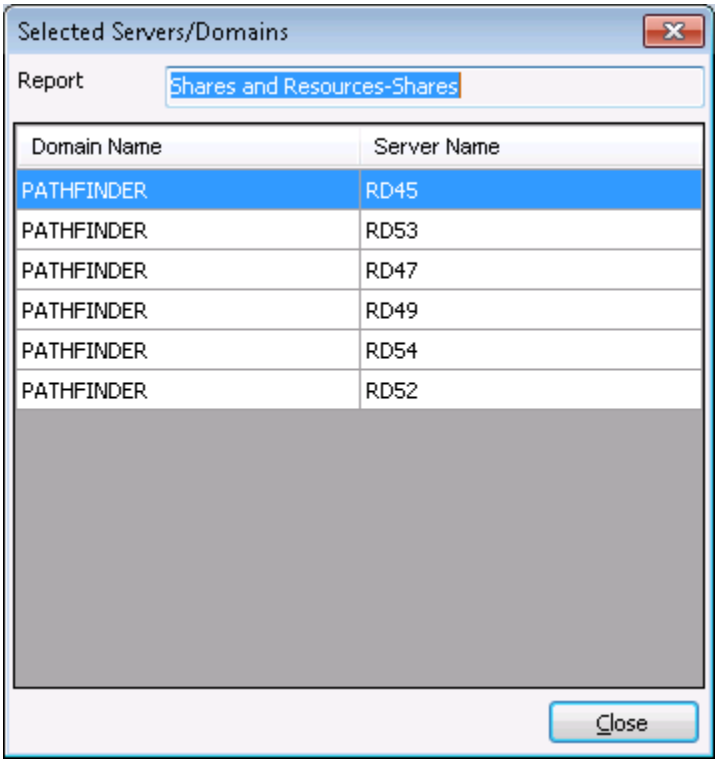
View summary information of a task

The pane on the left hand side in the Scheduled Tasks Manager window lists the tasks maintained in NTFS Security Auditor. To view summary information of a task, select the desired task on the left pane. The summary information of the selected task will be displayed in the right pane as shown below:



The task summary includes information about the task information, reports selected, export/print settings.

To view the selected servers/domains for a report in the task, click on the hyperlink in the **Servers/Domains** column in the right pane. The **Selected Servers/Domains** window will be displayed as shown below:



View exported files

To view the reports generated and exported by the task, perform either one of the following steps:

- Select Scheduled Tasks node on the left pane, and then click on the hyperlink in the Exported Files column in the right pane for the desired task.

OR

- Select the desired task on the left pane, and then click on the hyperlink next to Exported Files.

Edit Task

Select a task from the Scheduled Tasks Manager Window and Click Edit Task.

Perform the steps as in Schedule Shares, Folders and Files or Schedule Built-in Report based on the scheduled report type. While proceeding through the wizard you may change the settings, add a new report, delete a report, edit a report, change the export path etc.

The new settings will be used when the task runs the next time.

Delete Task

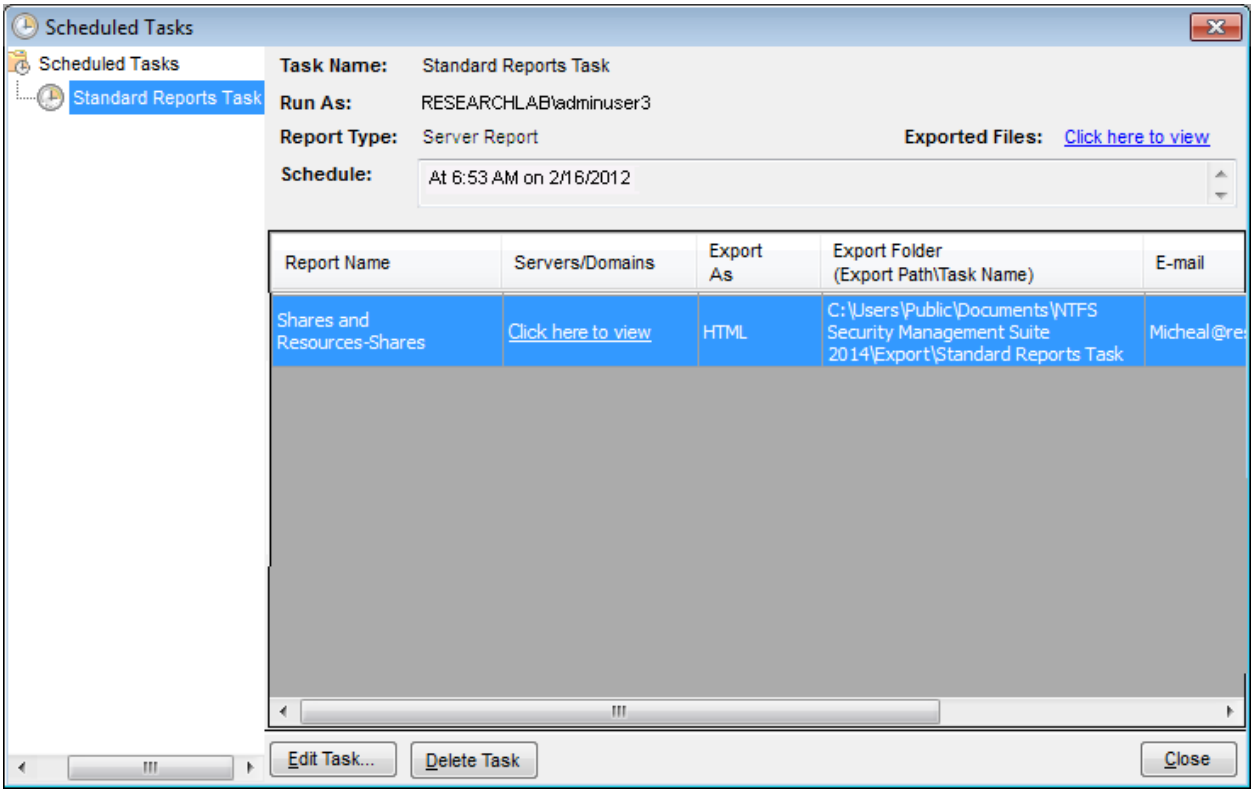
To delete a task from the Power Reports Task Manager Window, select the task and Click Delete Task. The deleted task will be removed permanently from the Windows Task Scheduler.

Task Status

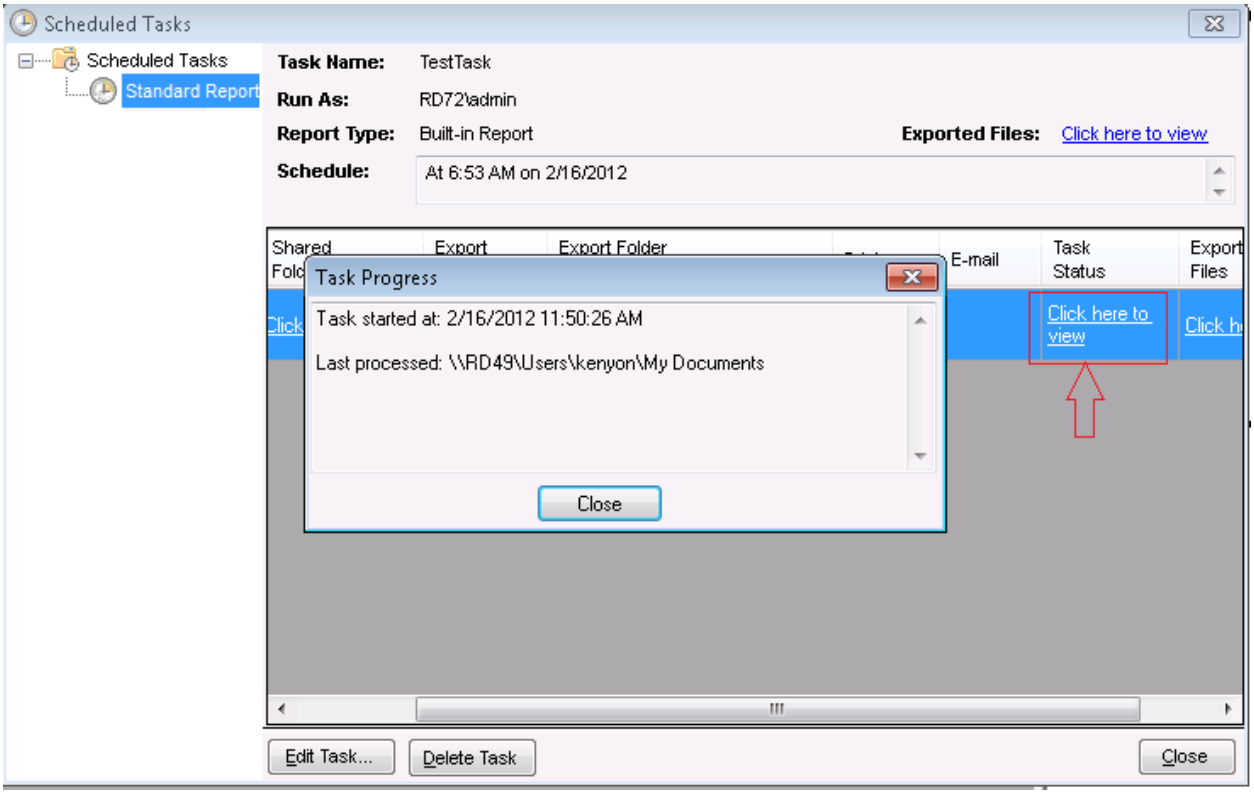
While running Power Export task configured with permissions reports, you may need to know the status of the tasks like last folder being processed, task start time, task complete status. For viewing this details, you can use the Task Status option. This option is especially useful when the schedule task is created in one user context other than currently logged user context.

For knowing the status of the running permission report task, perform the following steps:

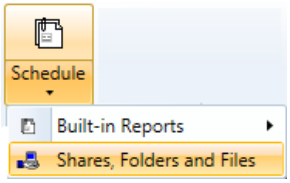
1. Select a permission report task from the Scheduled Tasks Manager Window.
2. The permission report task will be displayed as shown below



3. To view the selected folder(s)/ file(s) path being processed (task running), click on the hyperlink over the Task Status column in the right pane. The Task Status window will be displayed showing the folder(s)/ file(s) path being processed as shown below:

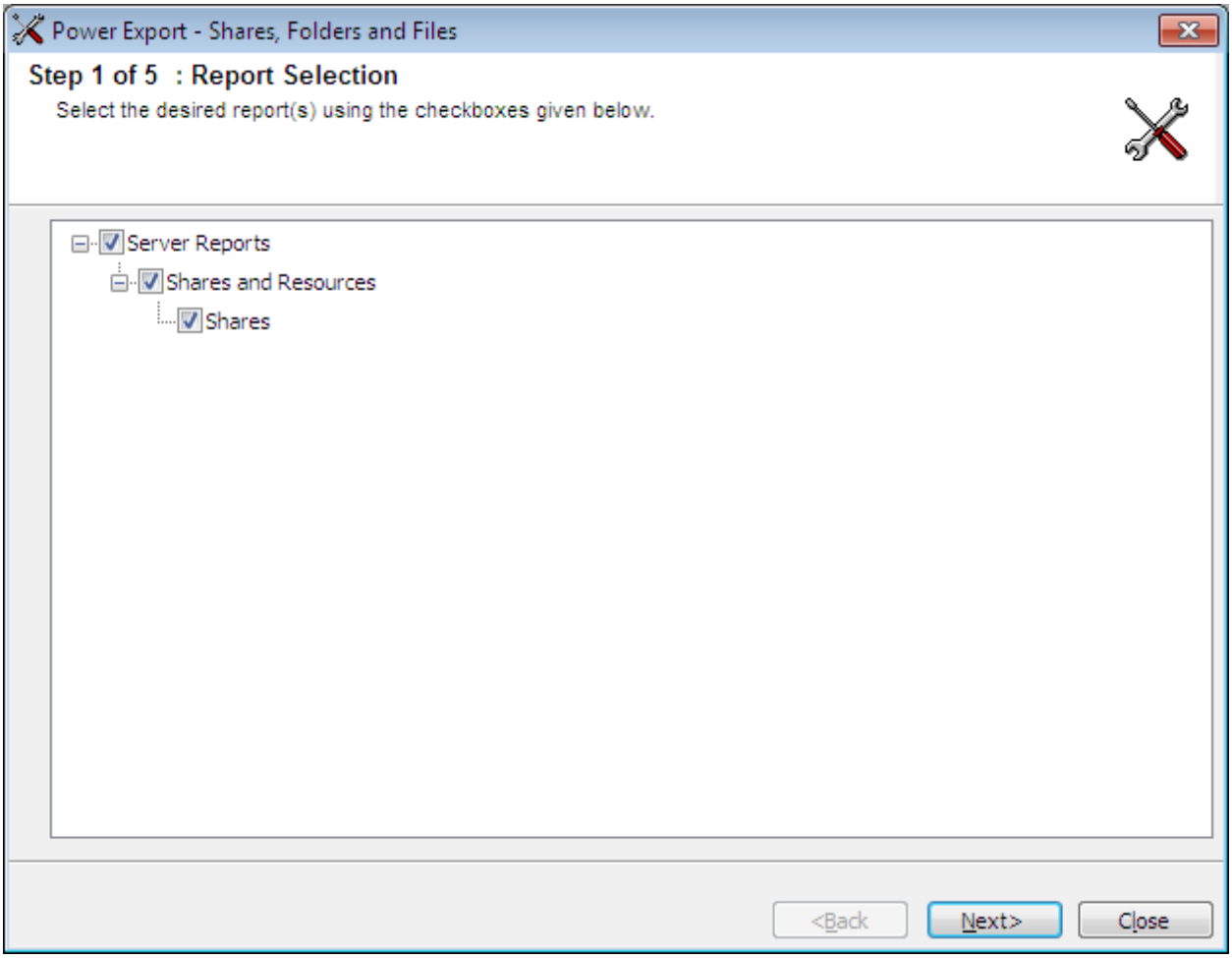

Scheduled Tasks
Scheduled Tasks
Standard Report
Task Name: TestTask
Run As: RD72\admin
Report Type: Built-in Report
Exported Files: Click here to view
Schedule: At 6:53 AM on 2/16/2012
Shared Fold
Export
Export Folder
E-mail
Task Status
Export Files
Click here to view
Task Progress
Task started at: 2/16/2012 11:50:26 AM
Last processed: \\RD49\Users\kenyon\My Documents
Close
Edit Task...
Delete Task
Close

Schedule Shares, Folders and Files Reports



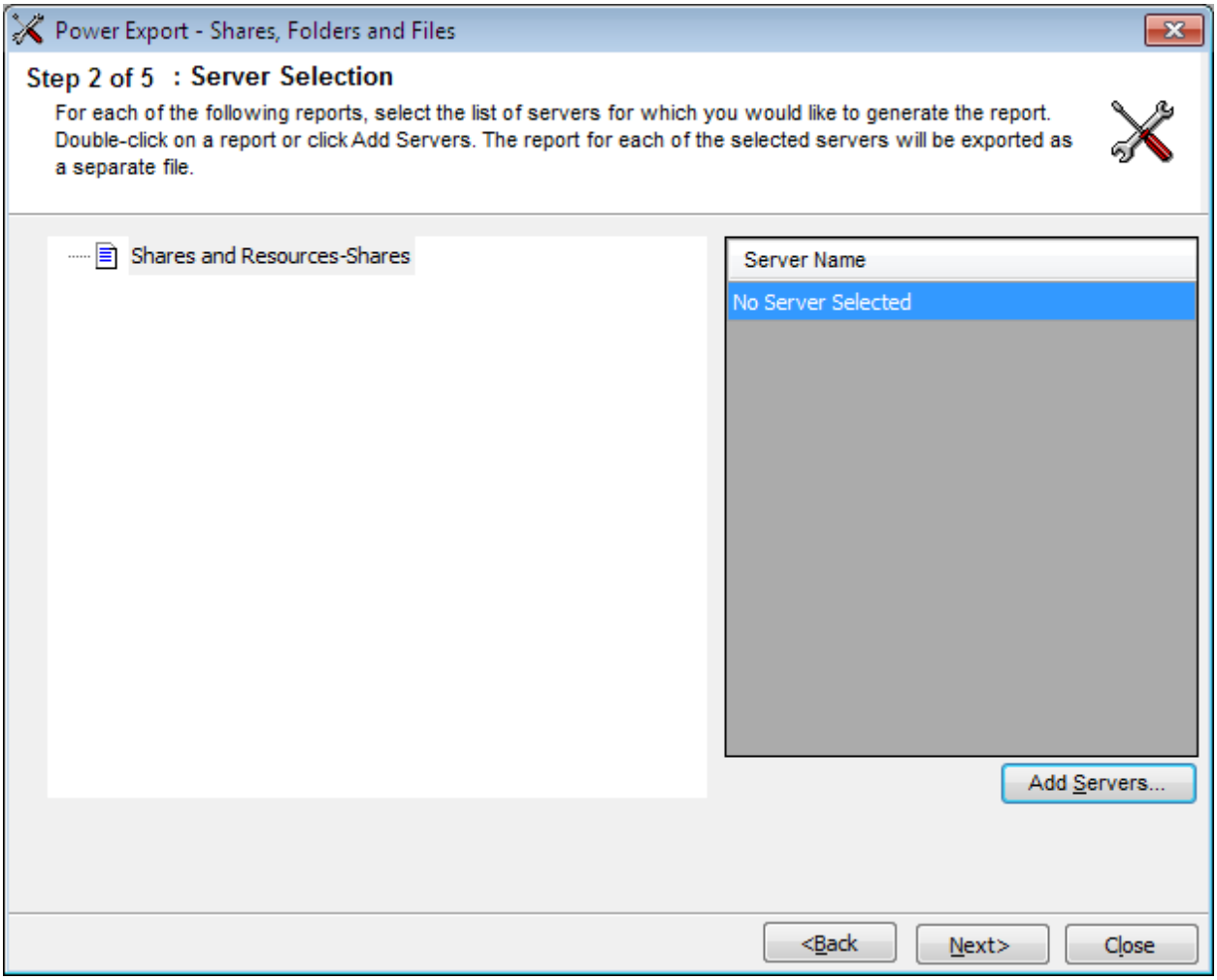
Select option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection

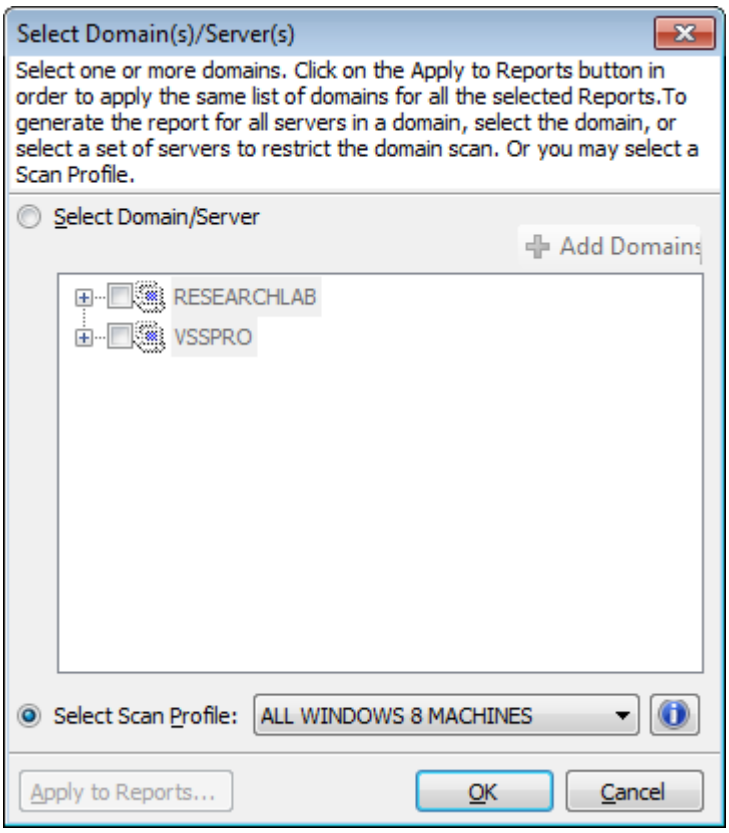

Power Export - Shares, Folders and Files
Step 1 of 5 : Report Selection
Select the desired report(s) using the checkboxes given below.
Server Reports
Shares and Resources
Shares
<Back
Next>
Close

1. Select the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
2. Reports falling under 'Server Reports' scan each server and collect data specific to each server. They are further classified by the category they report on (viz. Users, Policies, Events etc.).
3. Click Next to proceed to the next step. You may Click Back button anytime to come back to a previous step.

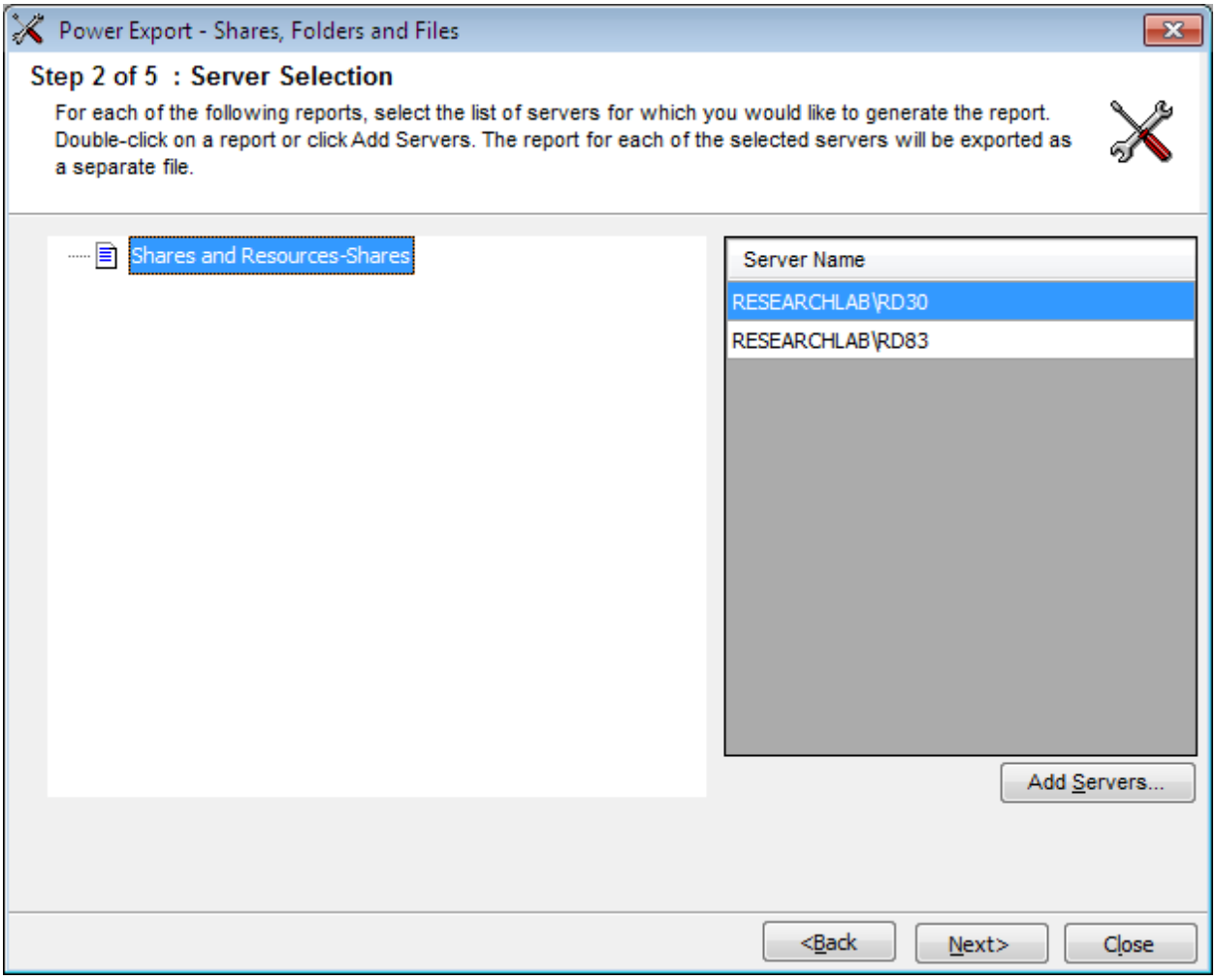
Step 2: Server Selection for Server Reports


Power Export - Shares, Folders and Files
Step 2 of 5 : Server Selection
For each of the following reports, select the list of servers for which you would like to generate the report. Double-click on a report or click Add Servers. The report for each of the selected servers will be exported as a separate file.
Shares and Resources-Shares
Server Name
No Server Selected
Add Servers...
<Back
Next>
Close

1. Click **Add Servers** button to select the servers for which you wish to run the server reports selected in Step 1. This will display a window where you can select the servers you want to add. Selecting a domain will add all the servers in that domain to the report.

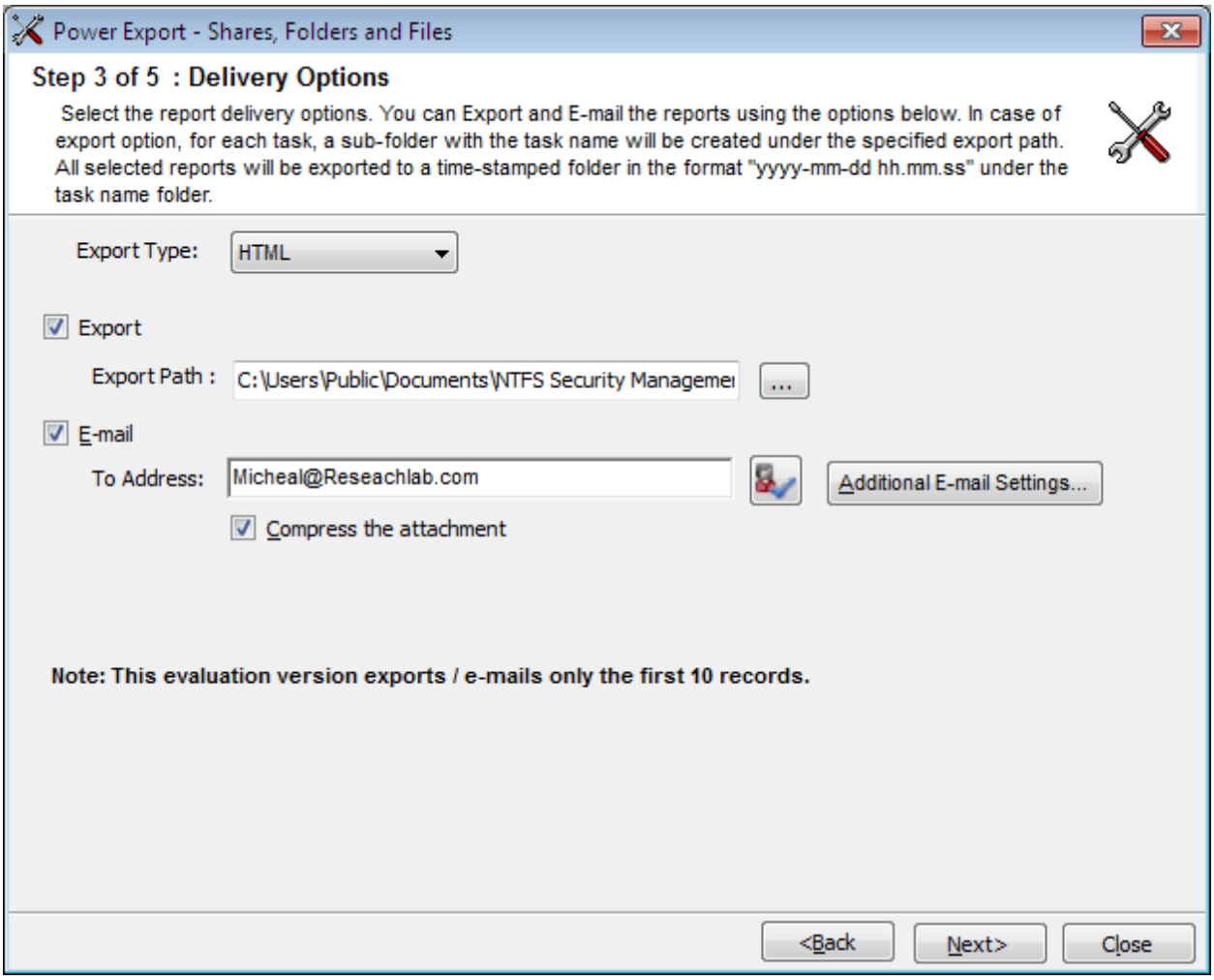

Select Domain(s)/Server(s)
Select one or more domains. Click on the Apply to Reports button in order to apply the same list of domains for all the selected Reports.To generate the report for all servers in a domain, select the domain, or select a set of servers to restrict the domain scan. Or you may select a Scan Profile.
Select Domain/Server
Add Domains
RESEARCHLAB
VSSPRO
Select Scan Profile:
ALL WINDOWS 8 MACHINES
Apply to Reports...
OK
Cancel

2. You can restrict the domain scope and scan and collect data only for a specific set of computers by either selecting specific computers under a domain or by selecting a Scan Profile.
3. Click **OK** to apply the selected servers or a Scan Profile to the current report or click **Apply** to Reports to apply the selection to the rest of the selected server reports. The selected servers will be added to the wizard as shown below.


Power Export - Shares, Folders and Files
Step 2 of 5 : Server Selection
For each of the following reports, select the list of servers for which you would like to generate the report. Double-click on a report or click Add Servers. The report for each of the selected servers will be exported as a separate file.
Shares and Resources-Shares
Server Name
RESEARCHLAB\RD30
RESEARCHLAB\RD83
Add Servers...
<Back
Next>
Close

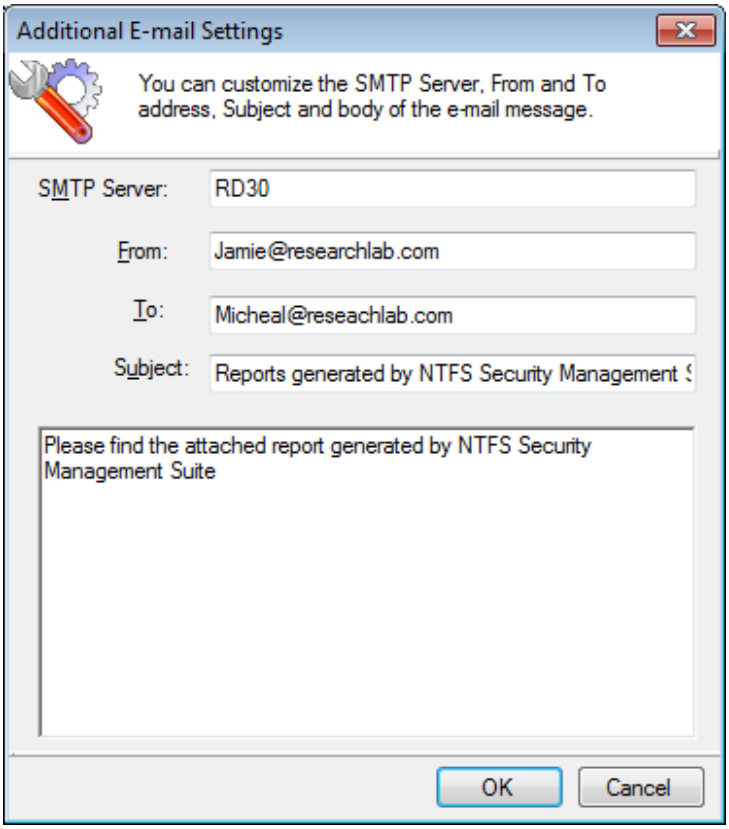
4. Click **Next** to proceed to the next Step.

Step 3: Delivery options

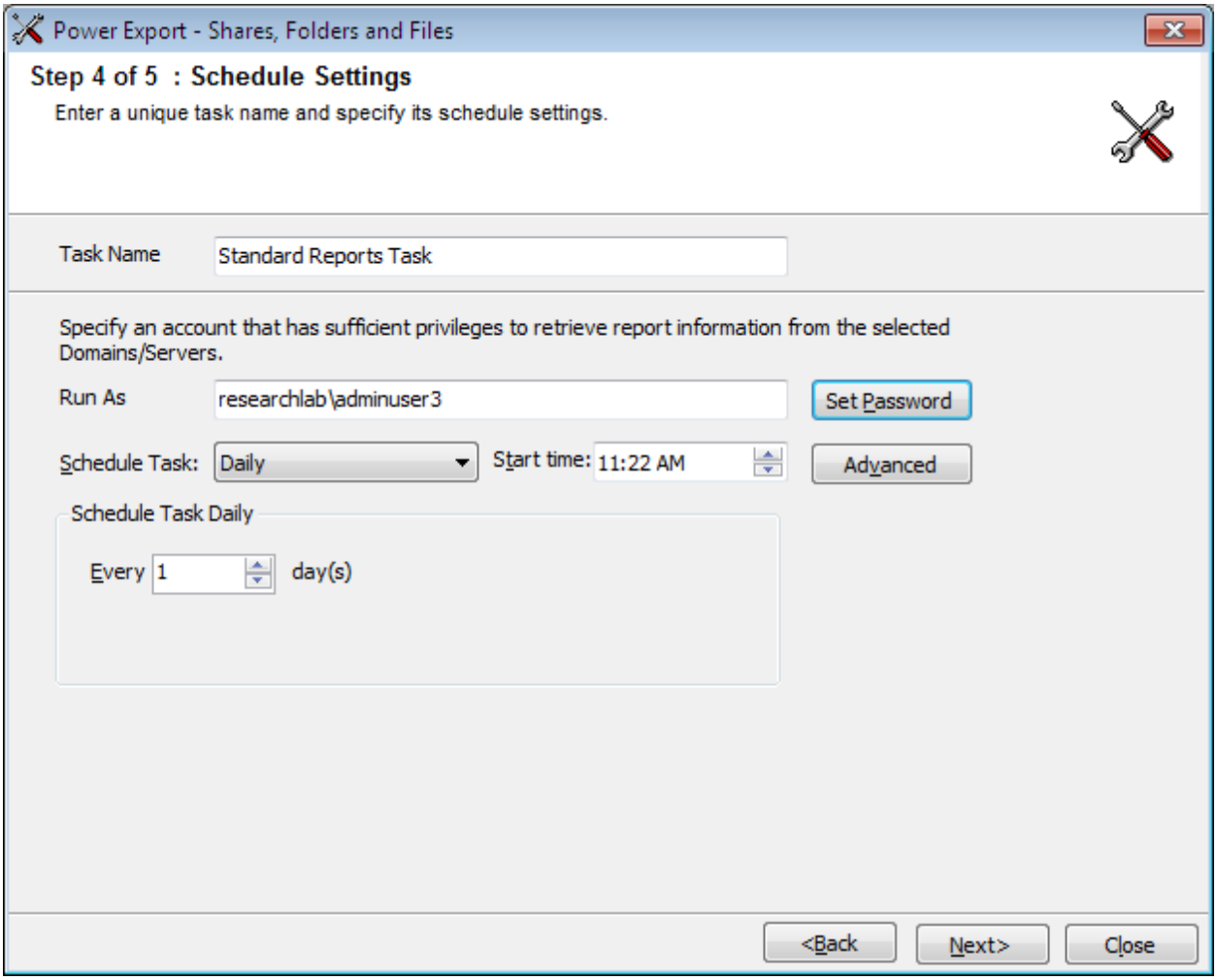

Power Export - Shares, Folders and Files
Step 3 of 5 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path

Click Additional E-mail Settings button to specify optional e-mail settings as shown below.


Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management S
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 4: Schedule Settings



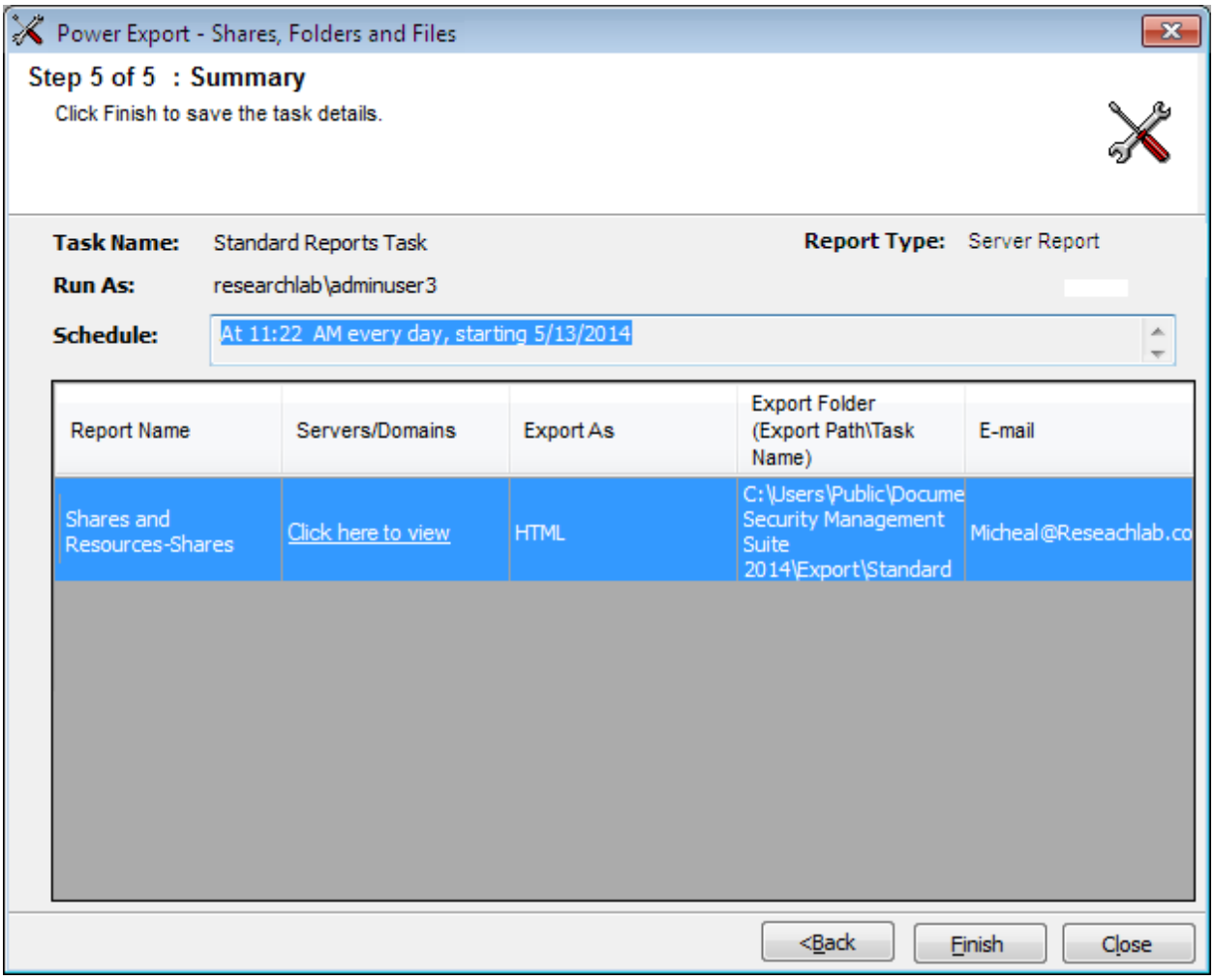
Enter a unique name for the task.

Change the Run as parameter, if necessary and set the password for the specified user.

Change the task schedule settings as required.

Click Next to proceed to the next and final step.

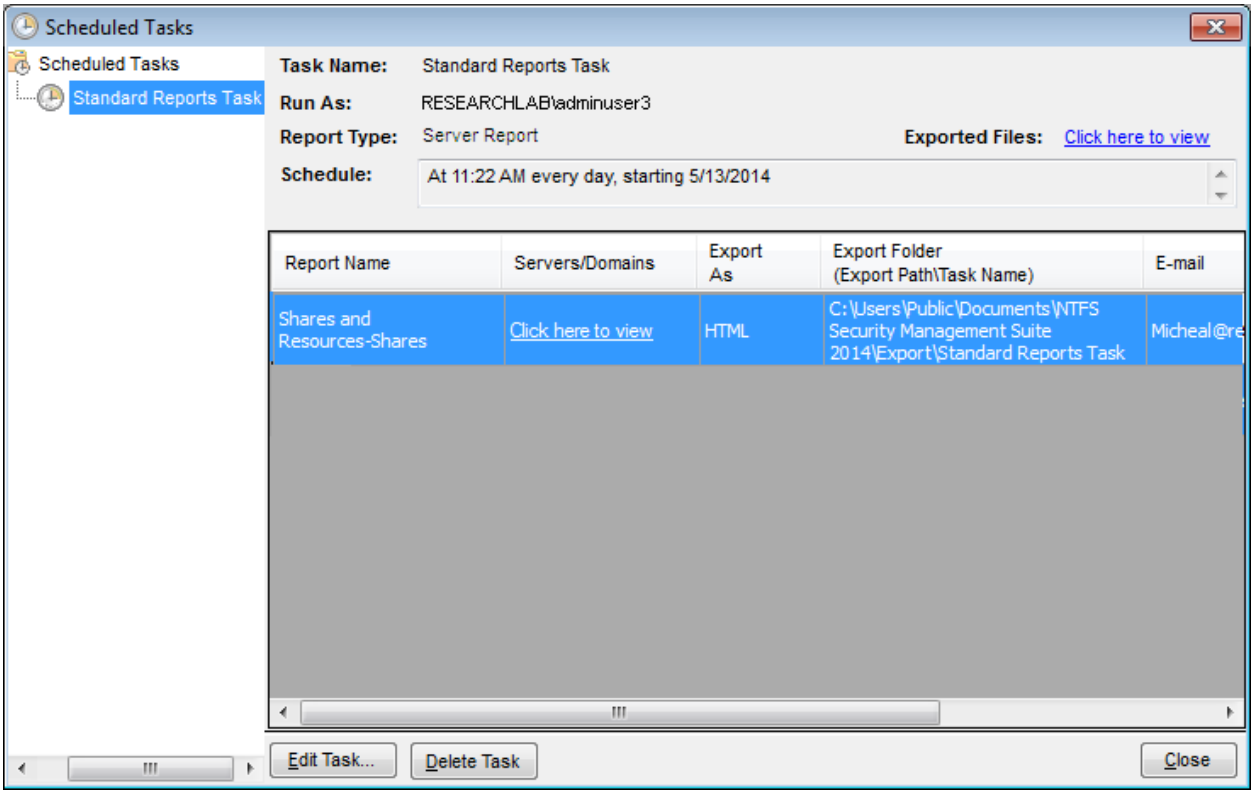
Step 5: Summary



This step displays the summary information of the task.

Click Finish to save the task details.

The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:


Scheduled Tasks
Scheduled Tasks
Standard Reports Task
Task Name: Standard Reports Task
Run As: RESEARCHLAB\adminuser3
Report Type: Server Report
Exported Files: Click here to view
Schedule: At 11:22 AM every day, starting 5/13/2014
Report Name
Servers/Domains
Export As
Export Folder (Export Path\Task Name)
E-mail
Shares and Resources-Shares
Click here to view
HTML
C:\Users\Public\Documents\NTFS Security Management Suite 2014\Export\Standard Reports Task
Micheal@re
Edit Task...
Delete Task
Close

Schedule Built-in Reports

The built-in reports have been categorized to the following:

Permissions Reports

Shares and Resources reports

Schedule Permissions Built-in Reports

Permissions Reports

Permissions Reports includes reports that focus solely on reporting the access permissions assigned to users and groups on objects such as folders etcetera.

- List of permissions for specific users and groups on folders
- List of permissions for folders
- List of permissions for specific users and groups on files
- List of permissions for files
- List of all permissions for folders (Inherited & Explicit)
- List of effective permissions for users and groups on folders
- List of effective permissions for users and groups on files
- List of effective permissions for specific users and groups on folders
- List of effective permissions for specific users and groups on files

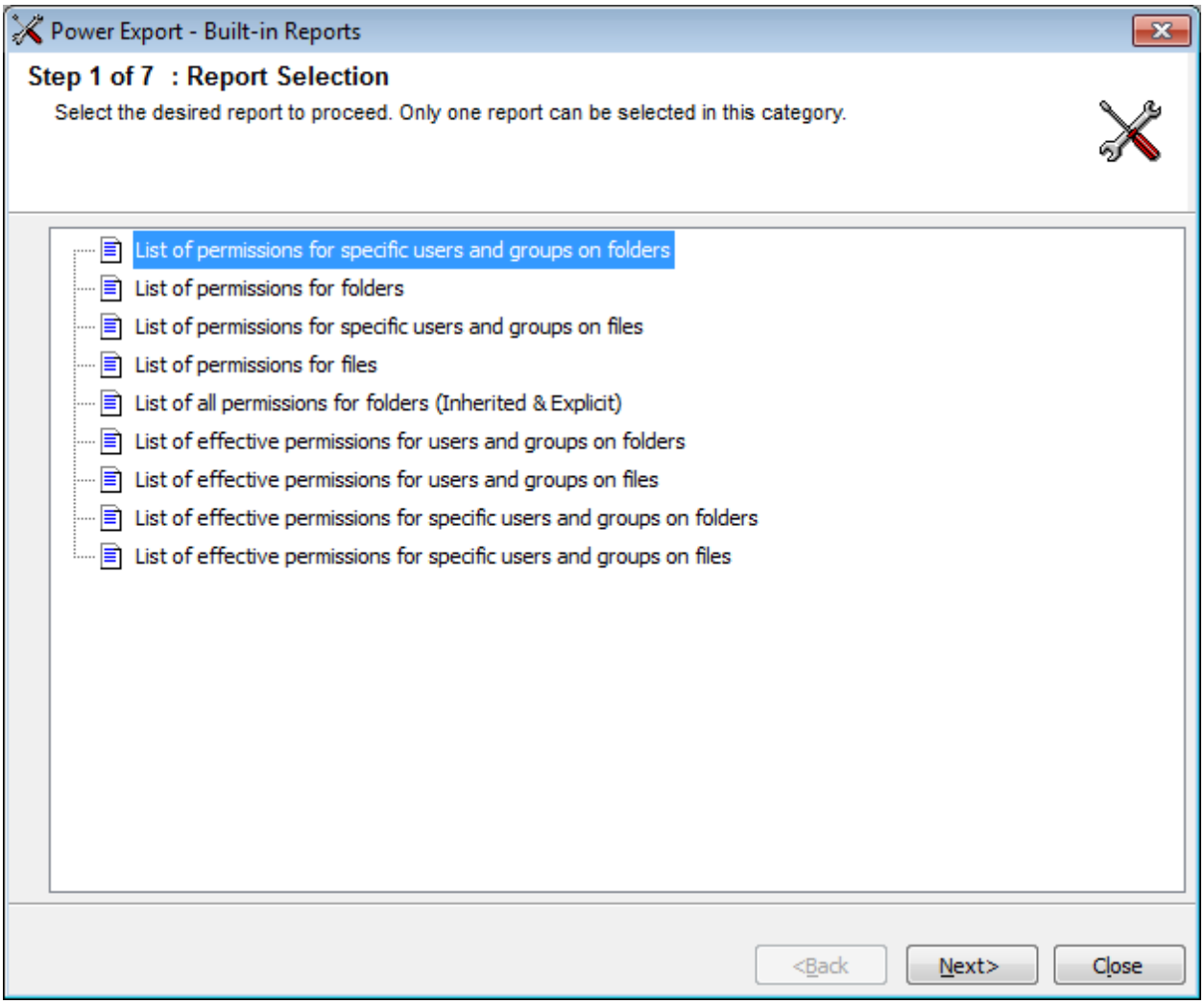
List of permissions for specific users and groups on folders

This report allows you to view folder permissions for specific users and groups.

Select

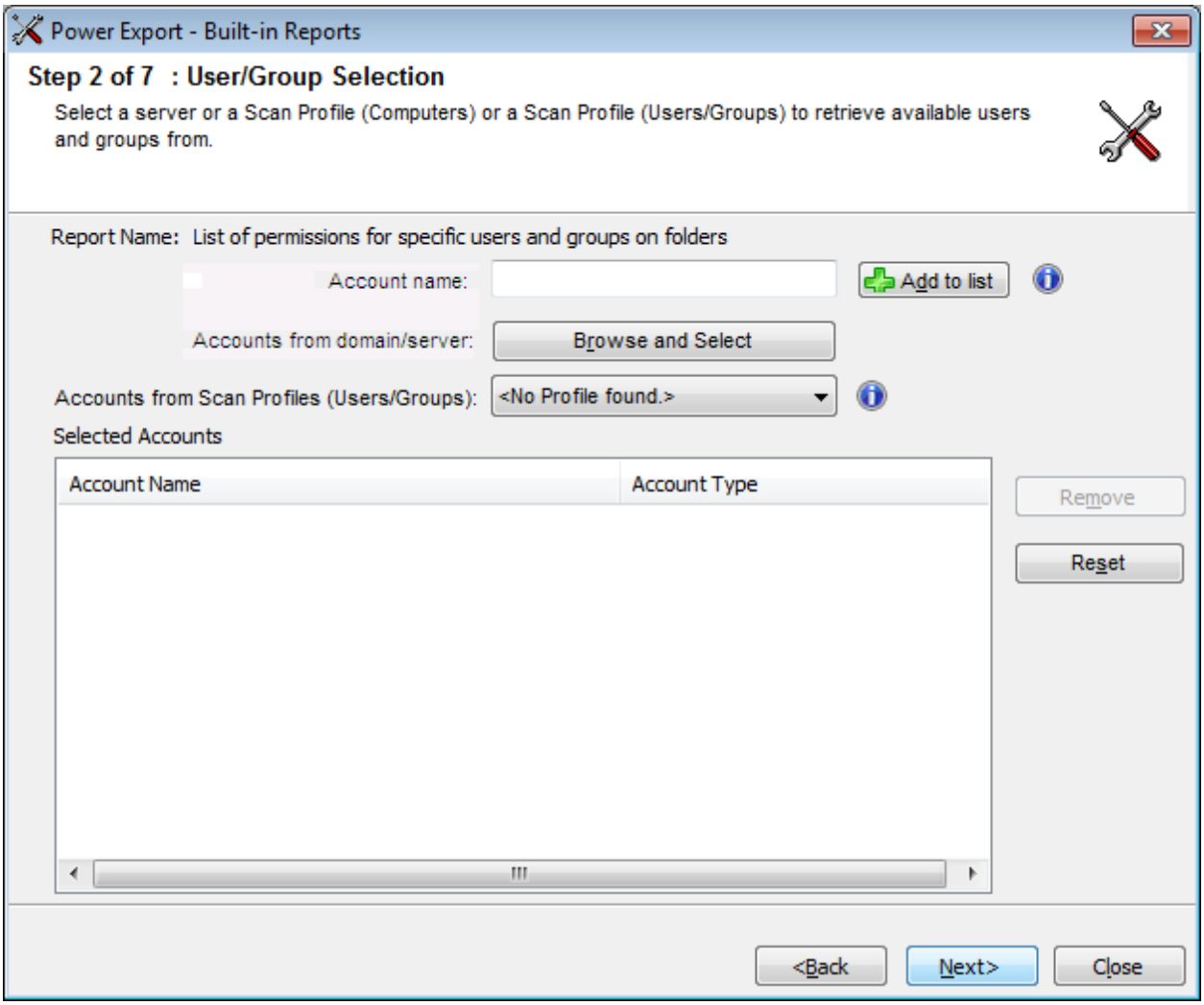
option under Power Export. This will bring up the Power Export Wizard.

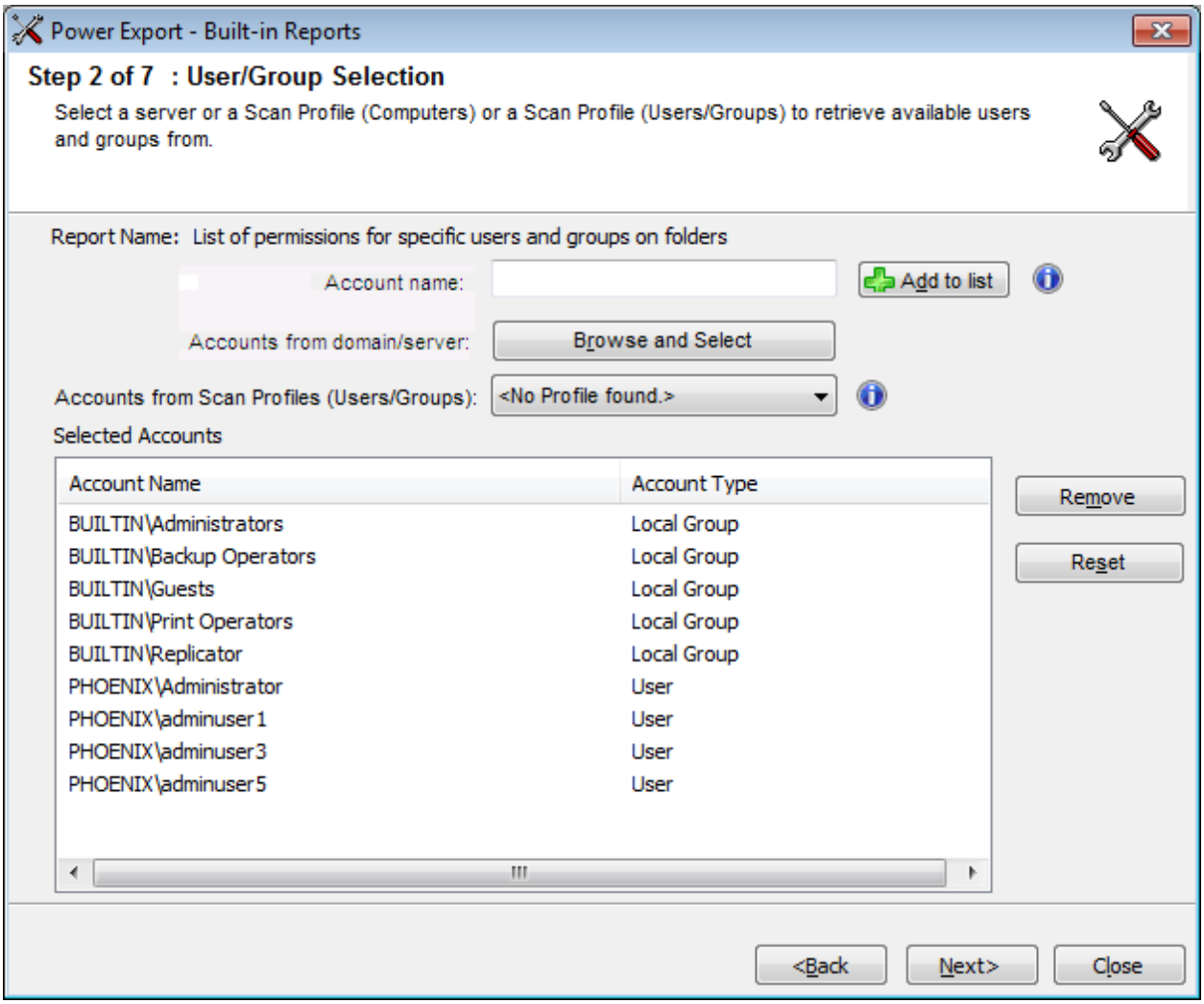
Step 1: Report Selection


Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: User and/or Group Selection

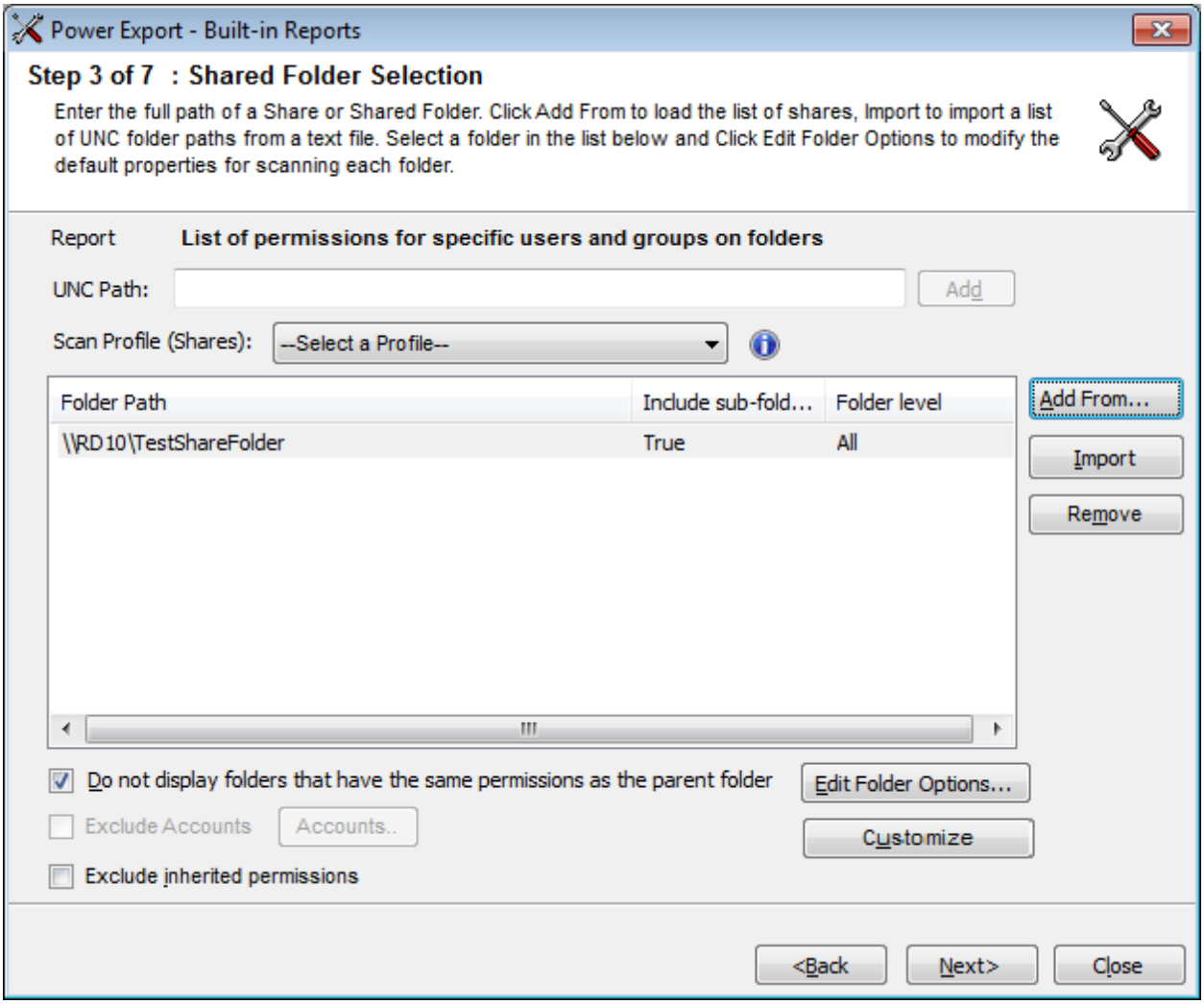

Power Export - Built-in Reports
Step 2 of 7 : User/Group Selection
Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.
Report Name: List of permissions for specific users and groups on folders
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
<No Profile found.>
Selected Accounts
Account Name
Account Type
Remove
Reset
<Back
Next>
Close



- Use Select a **Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

1. Select the user or group, for which you wish to run the permissions report.
2. The selected users will be added to the wizard as shown above:
3. Click Next to proceed to the Next step.

Step 3: Shared Folder Selection


Power Export - Built-in Reports
Step 3 of 7 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of permissions for specific users and groups on folders
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
Exclude inherited permissions
<Back
Next>
Close

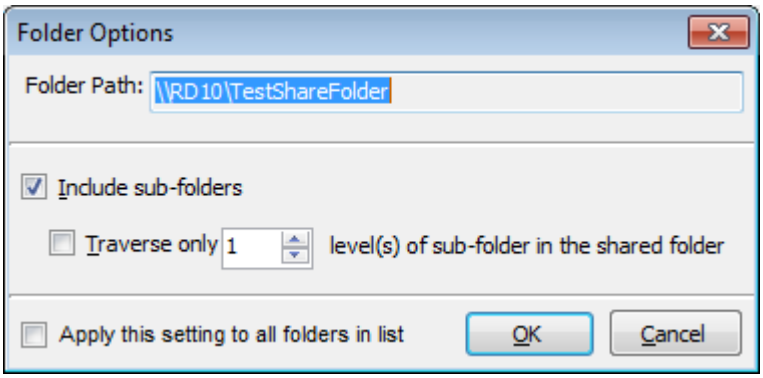
1. Select the desired folder(s) for which you wish to run the permissions report.

2. You may also click **Import** button to import a list of UNC folder paths from a text file.

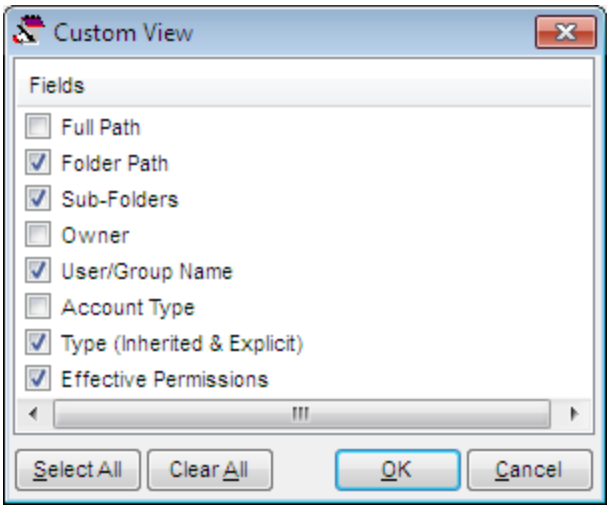
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button.

That will show up a window as shown below:



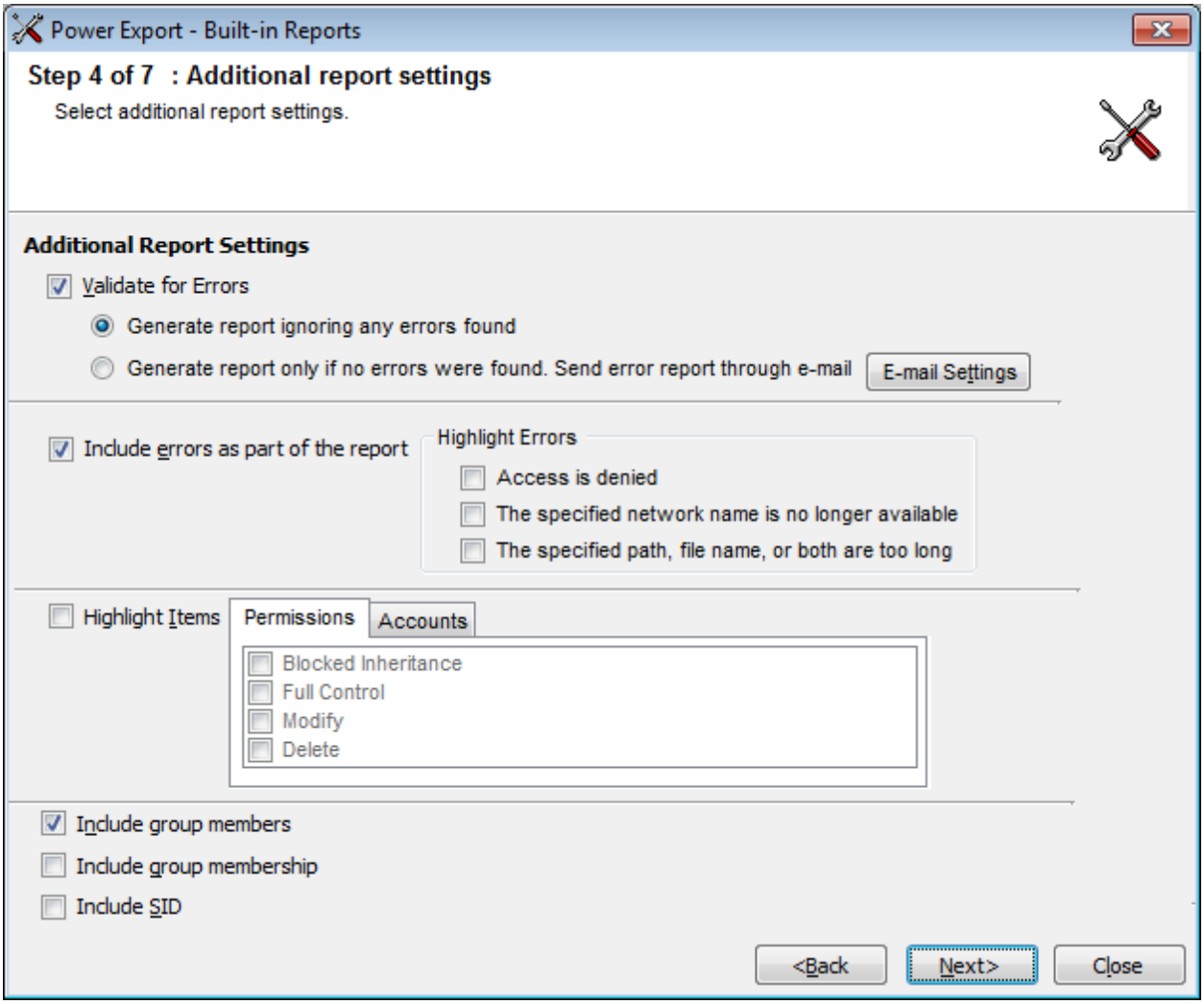
5. Modify the folder options as required and click **OK**.
6. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



7. Select the customize options as required and click **OK**.
8. You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.

9. Click **Next** to proceed to the Next step.

Step 4: Additional report settings



1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.

    - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
    - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.

2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.

3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

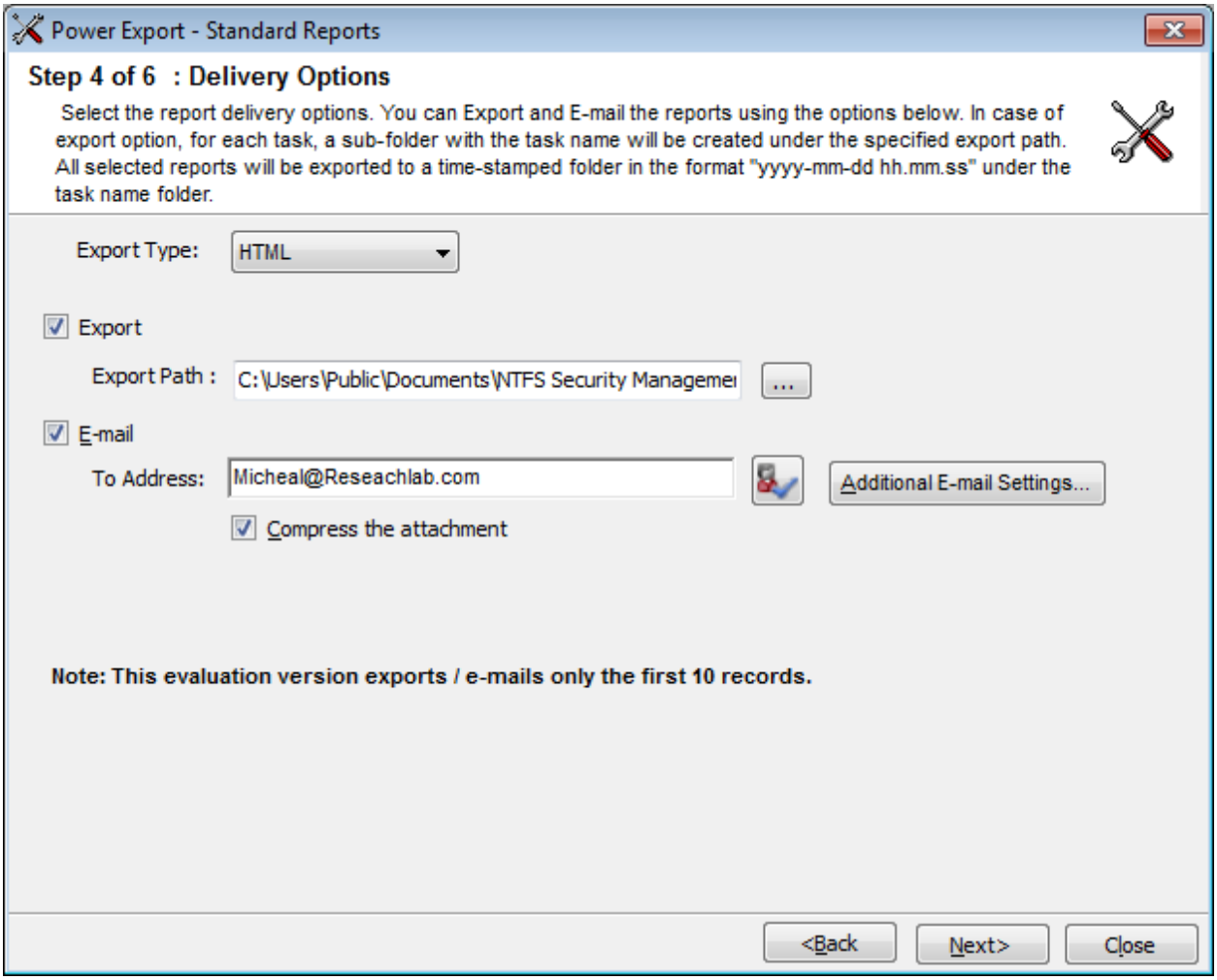
4. You may also select **Include group members** for include members of group and their sub-group members at all group levels in the report.

5. You may also select **Include group membership** for include membership information of user and group in the report.

6. You may also select **Include SID** for include SID value for user in the report.

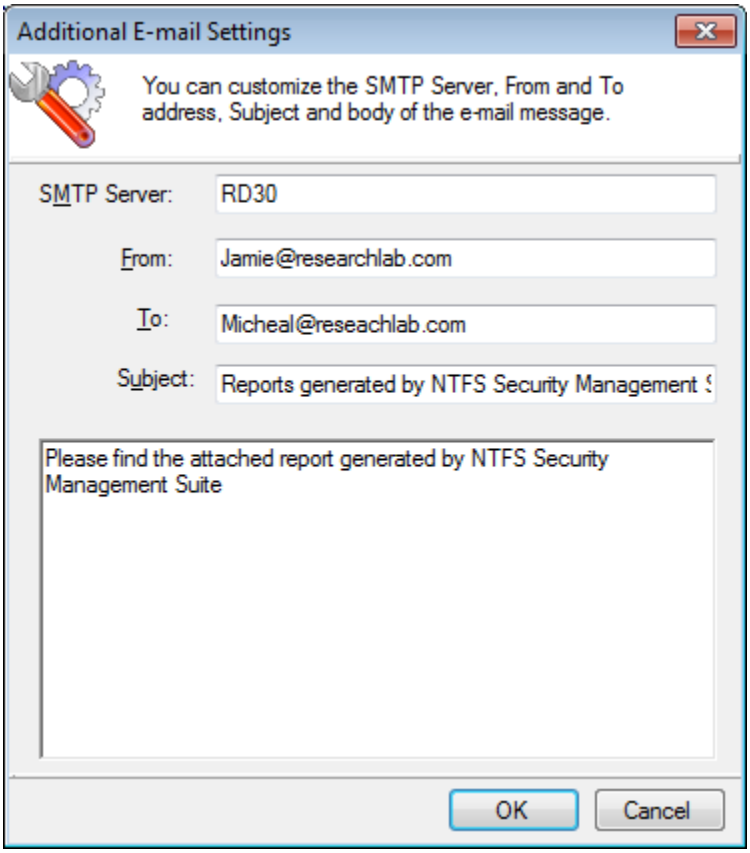
7. Click **Next** to proceed to the Next step.

Step 5: Delivery Options

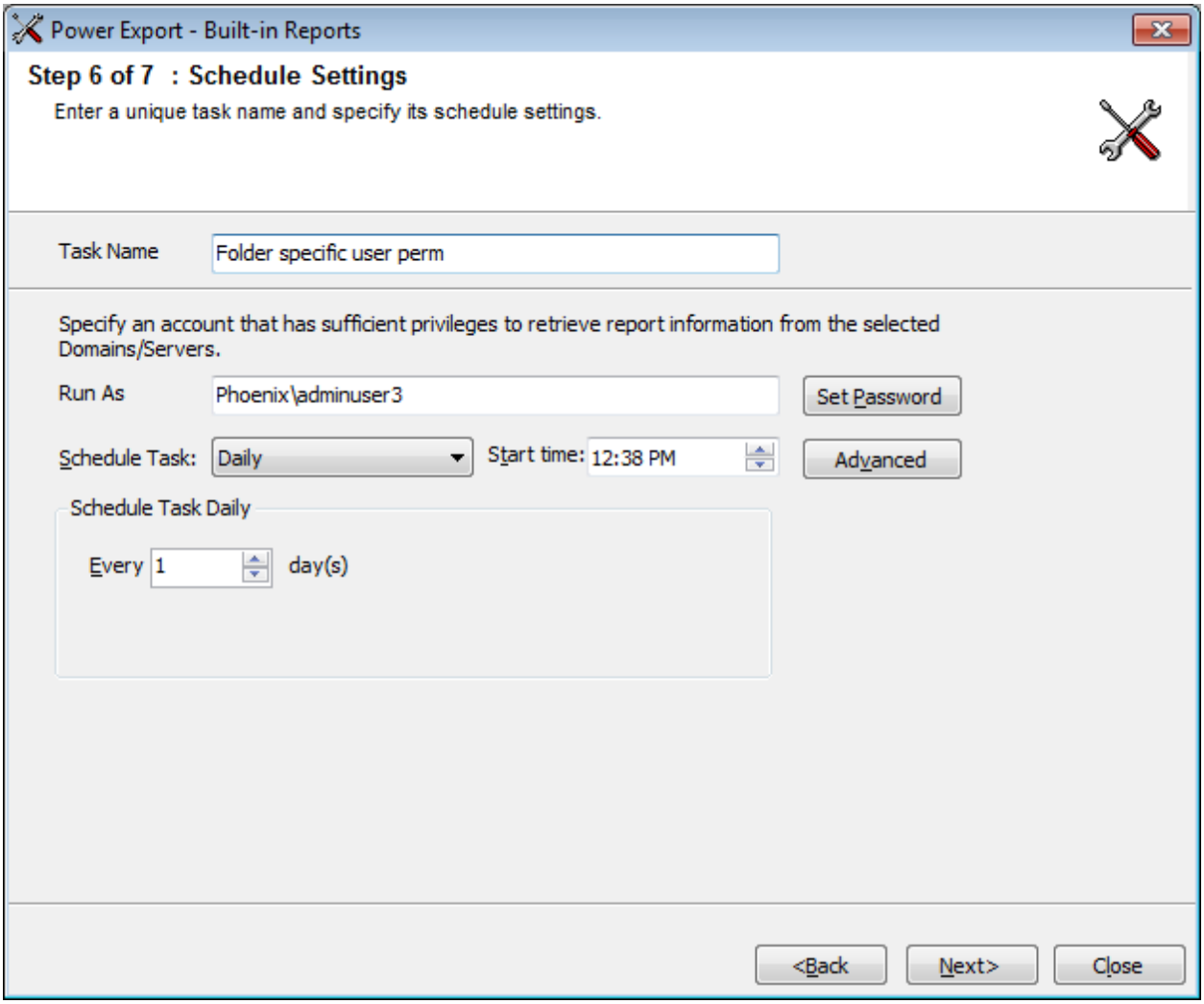

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail** Settings button to specify optional e-mail settings as shown below.

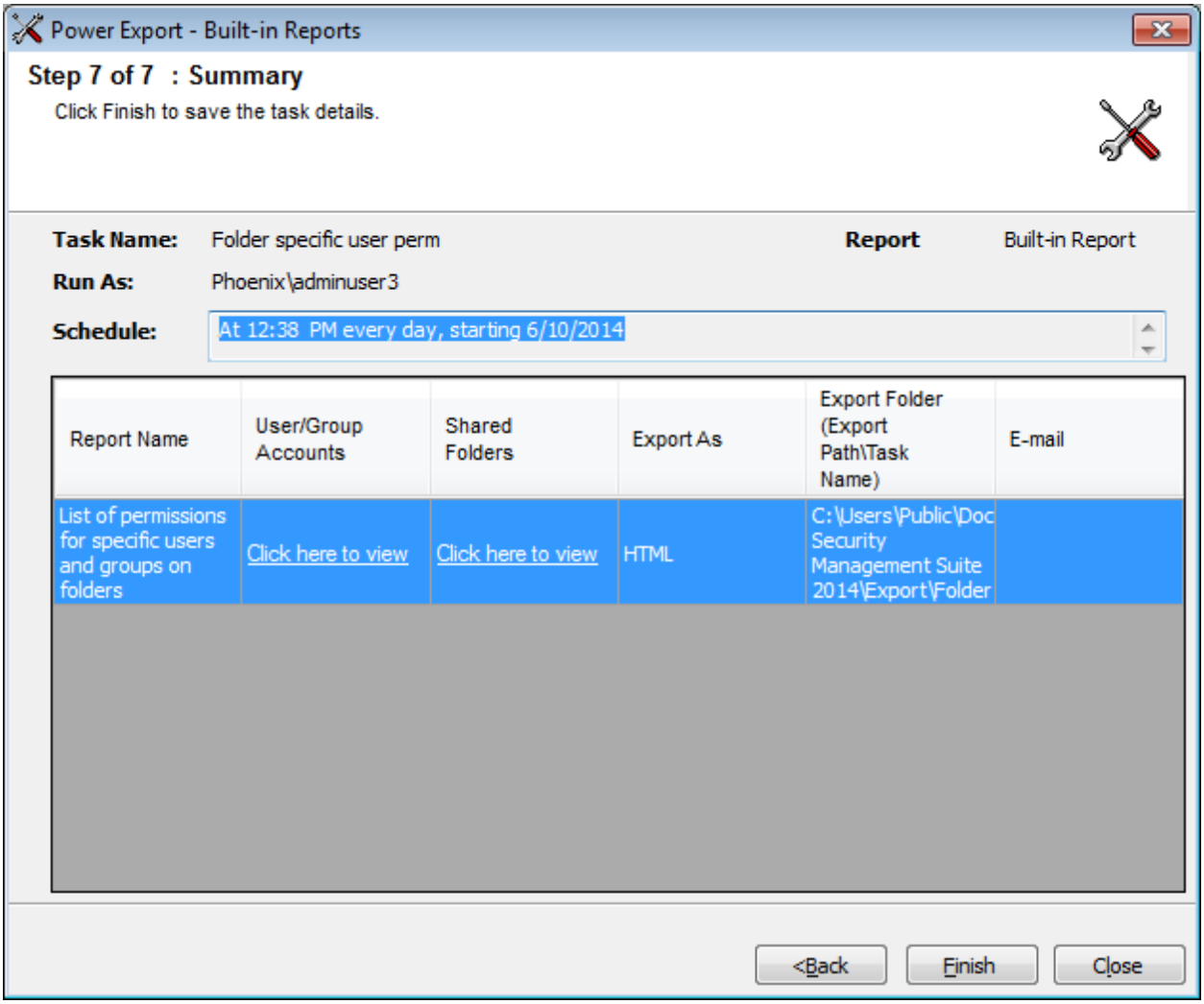

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 6: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 7: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

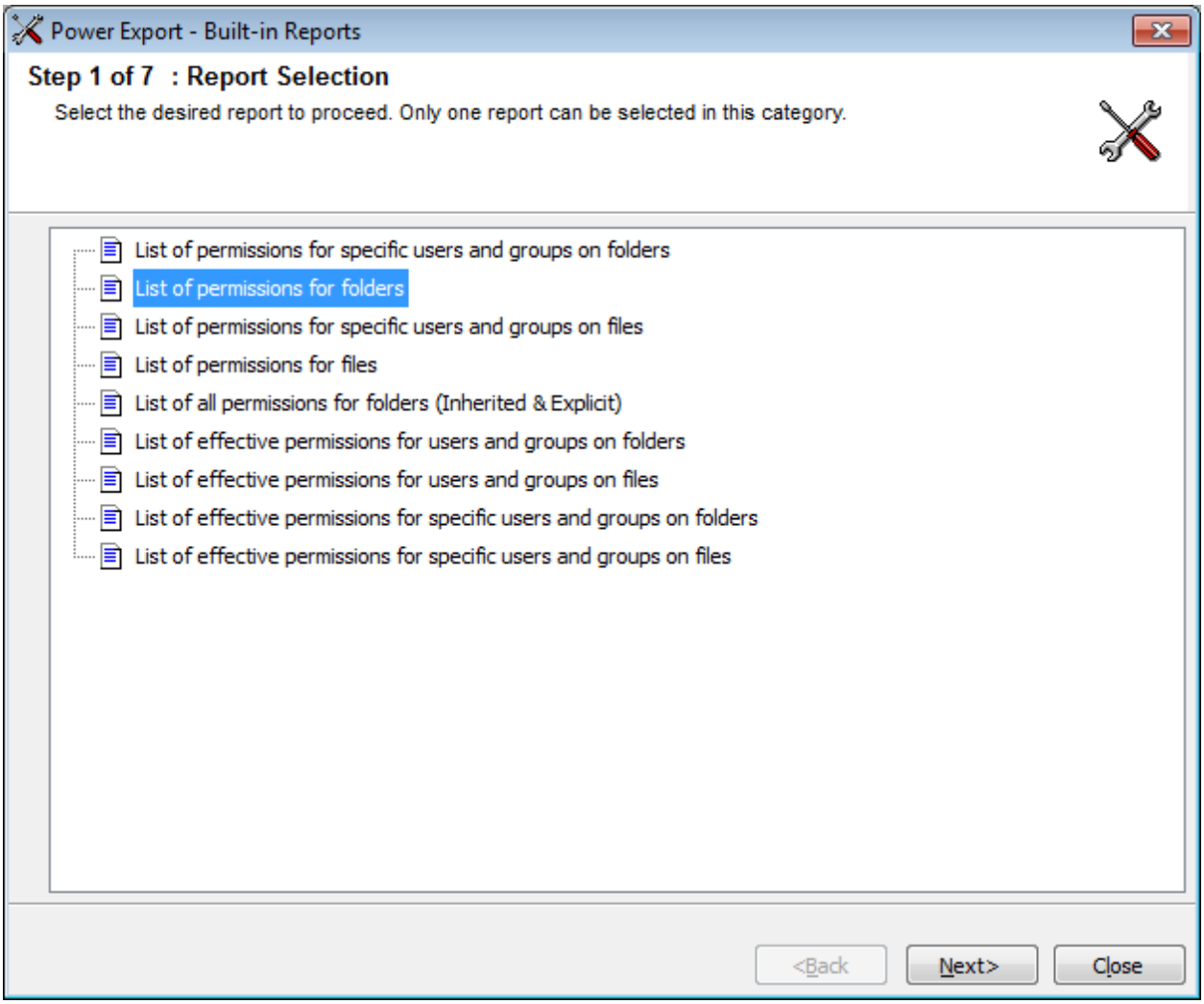
List of permissions for folders

This report, allows you to view the associated folder permissions for a set of folders.

Select

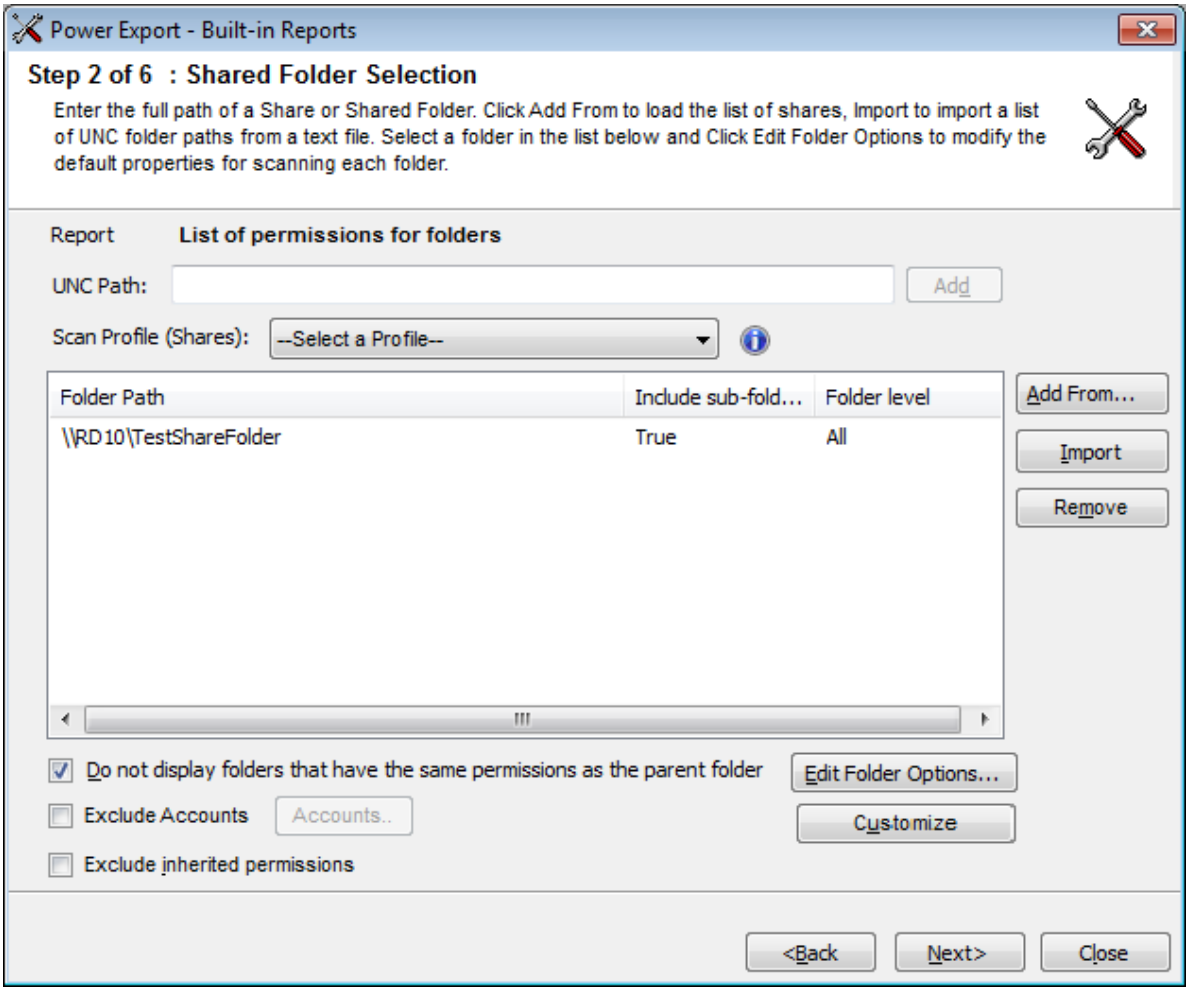
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection

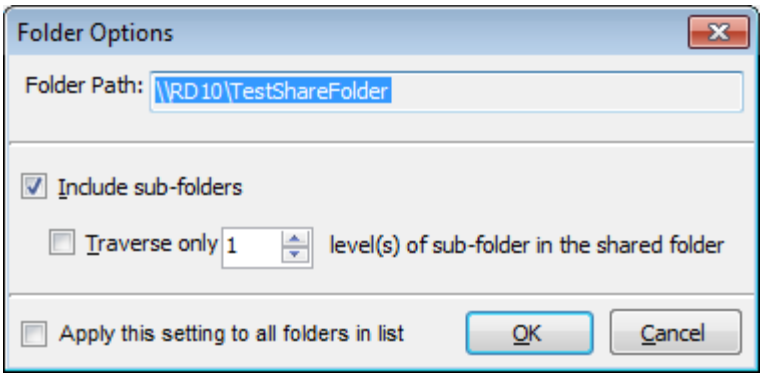

Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

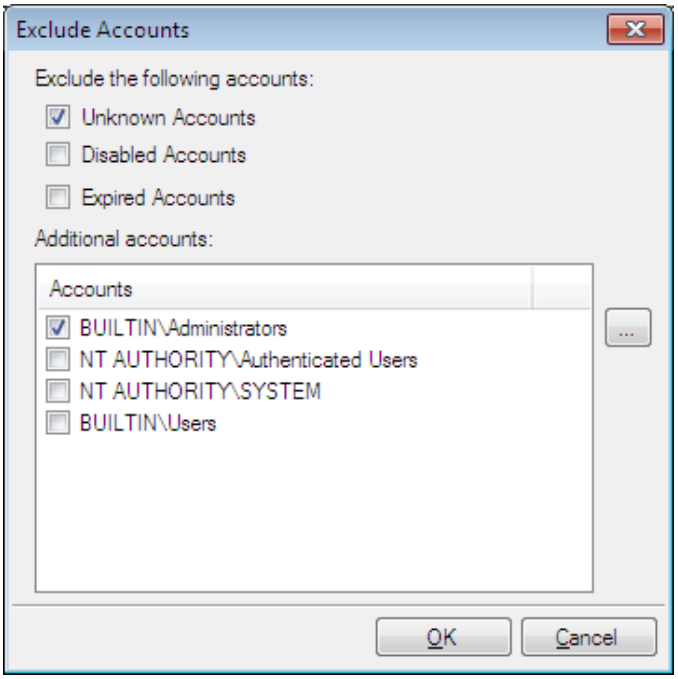
Step 2: Shared Folder Selection


Power Export - Built-in Reports
Step 2 of 6 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of permissions for folders
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
Exclude inherited permissions
<Back
Next>
Close

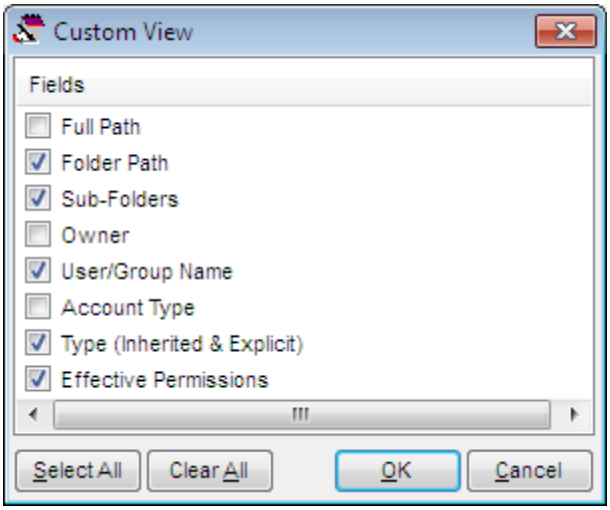
1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options button**. That will show up a window as shown below:



5. Modify the folder options as required and click **OK**.
6. If you want to exclude specific accounts select **Exclude Accounts** option. Click **Accounts...** button. That will show up a window as shown below:

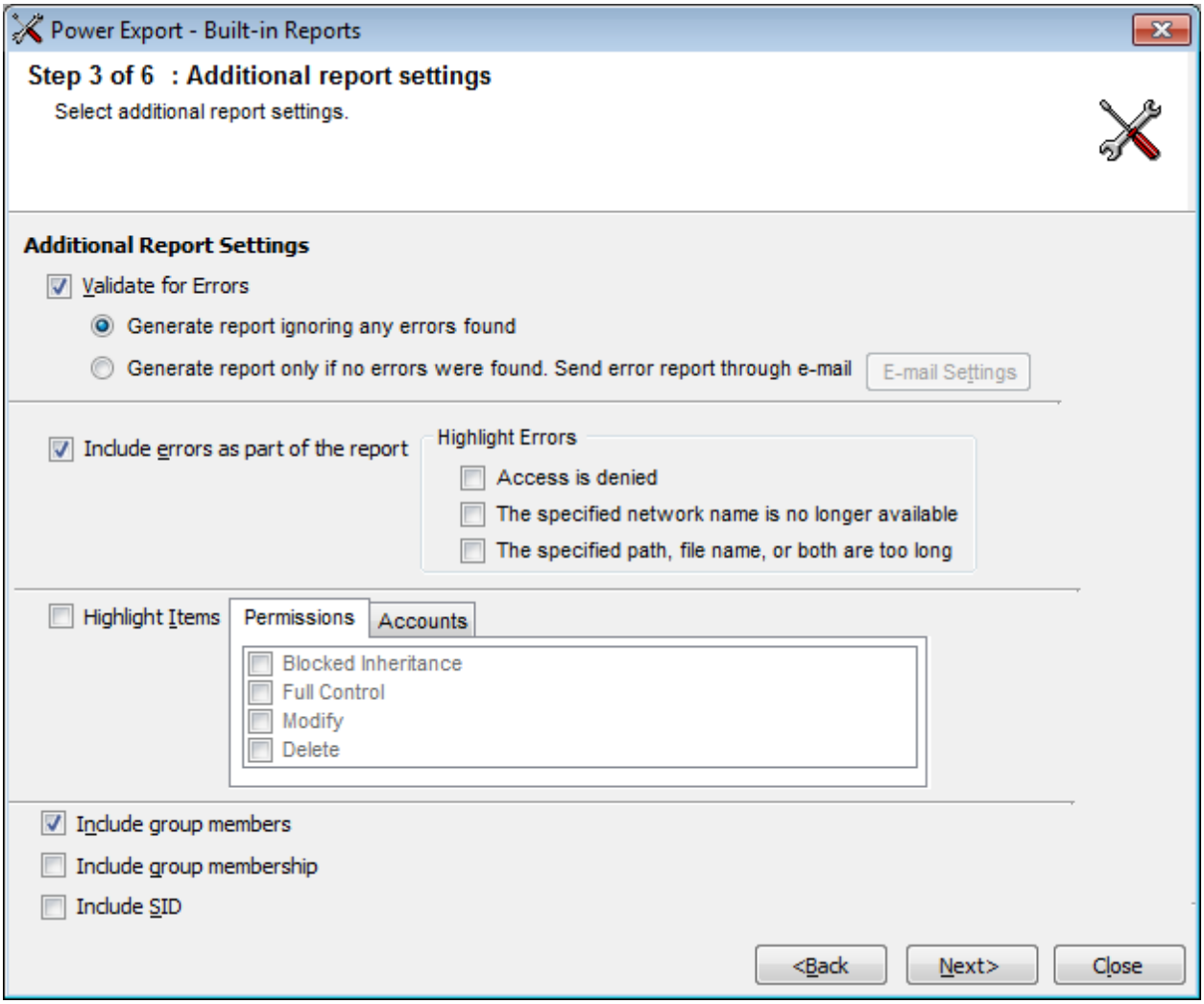


7. Select the accounts for which you want to exclude and click **OK**.
8. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



9. Select the customize options as required and click **OK**.
10. You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.
11. Click **Next** to proceed to the Next step.

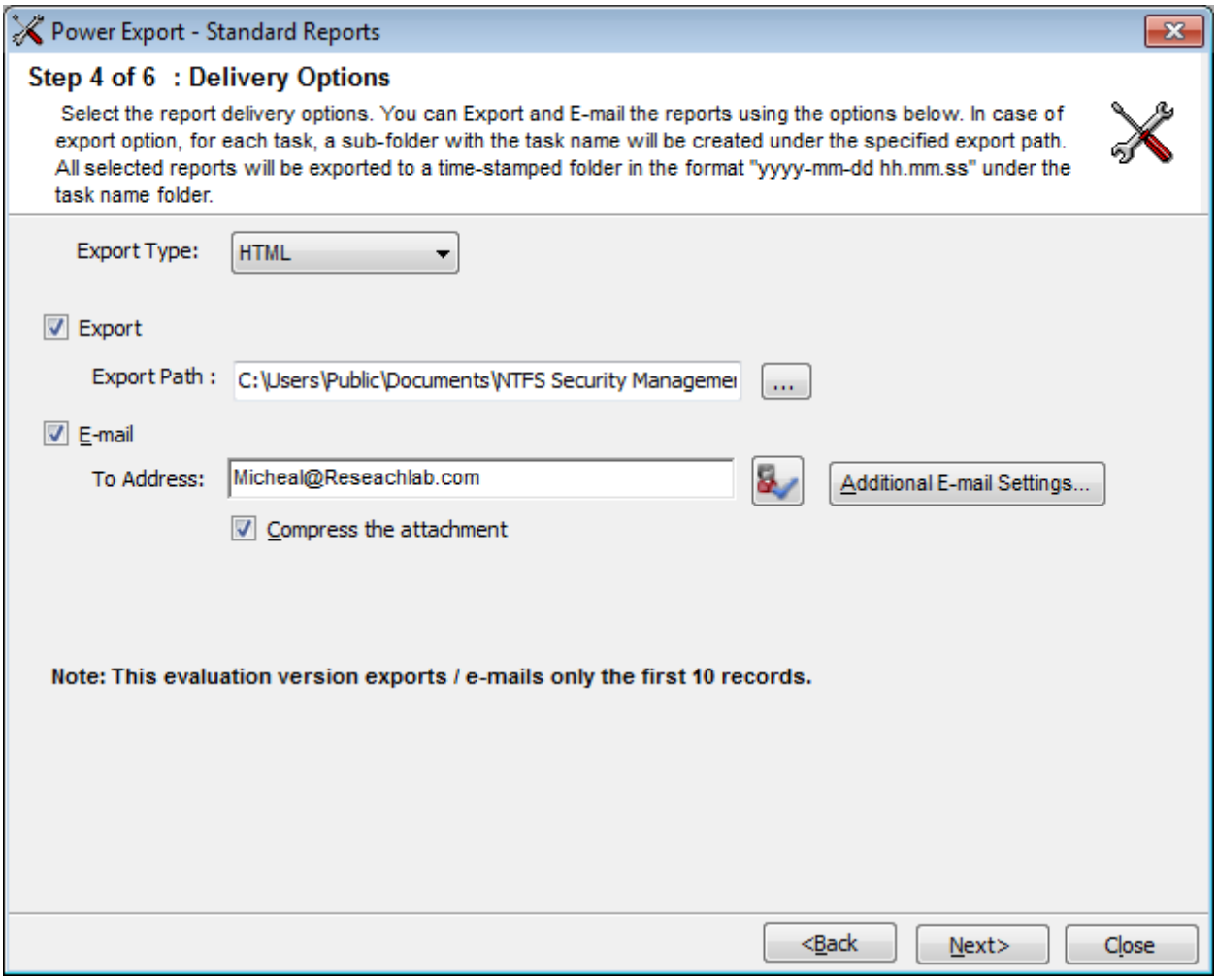
Step 3: Additional report settings



1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

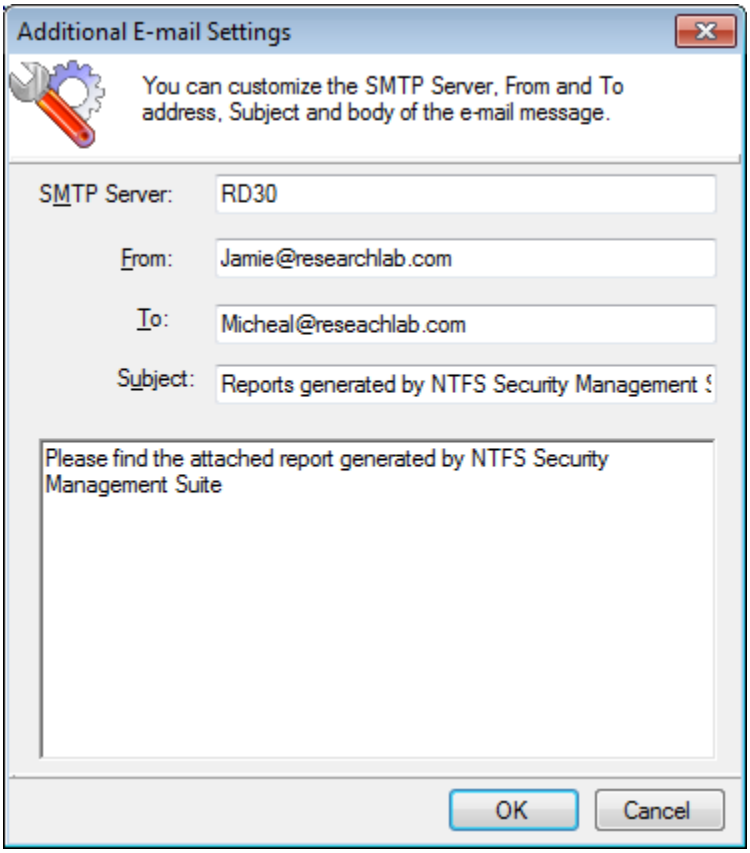
4. You may also select **Include group members** for include members of a group and their sub-group members at all levels in the report.
5. You may also select **Include group membership** for include membership information of user and group in the report.
6. You may also select **Include SID** for include SID value for user in the report.
7. Click **Next** to proceed to the Next step.

Step 4: Delivery Options

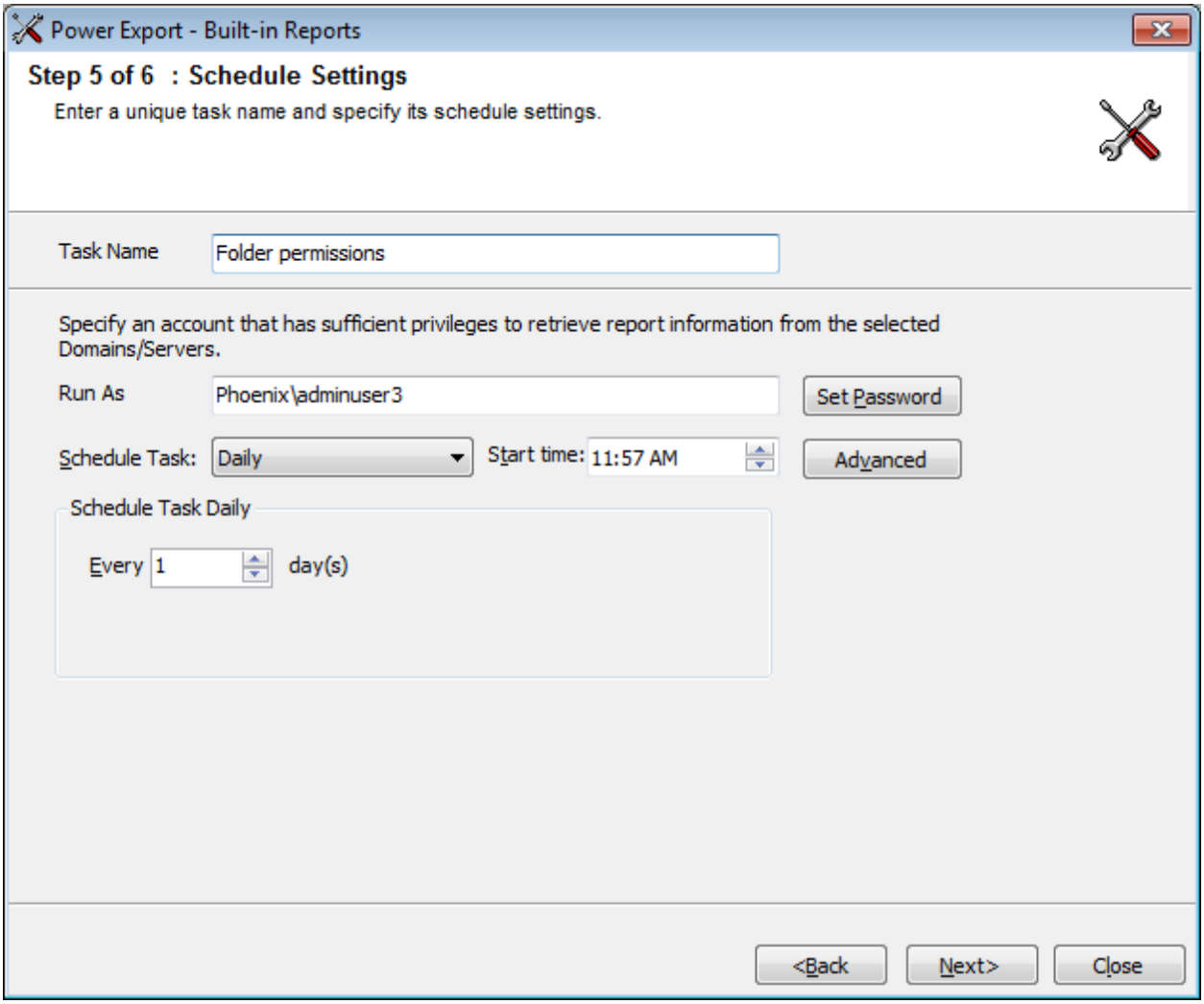

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail** Settings button to specify optional e-mail settings as shown below.

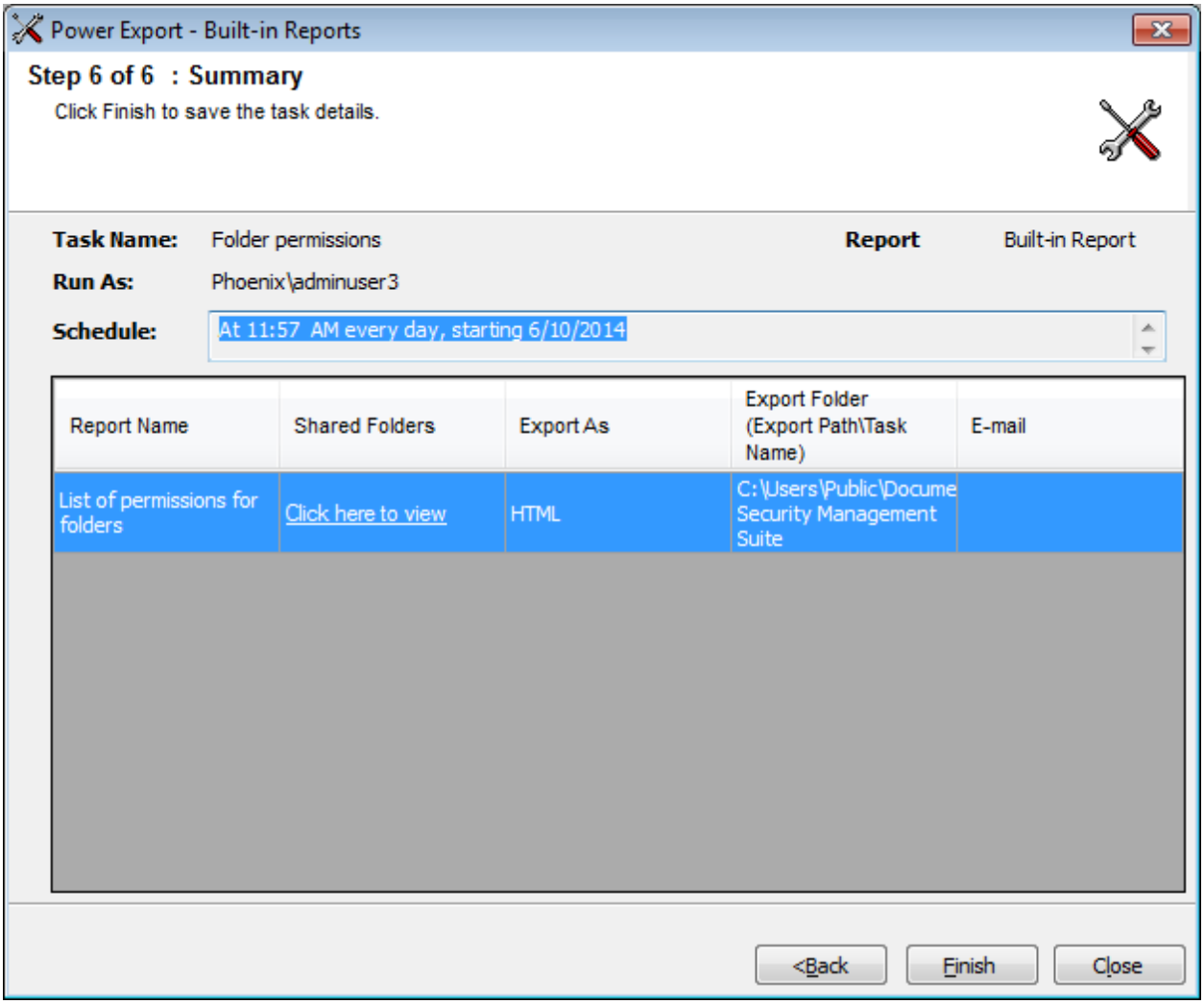


Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

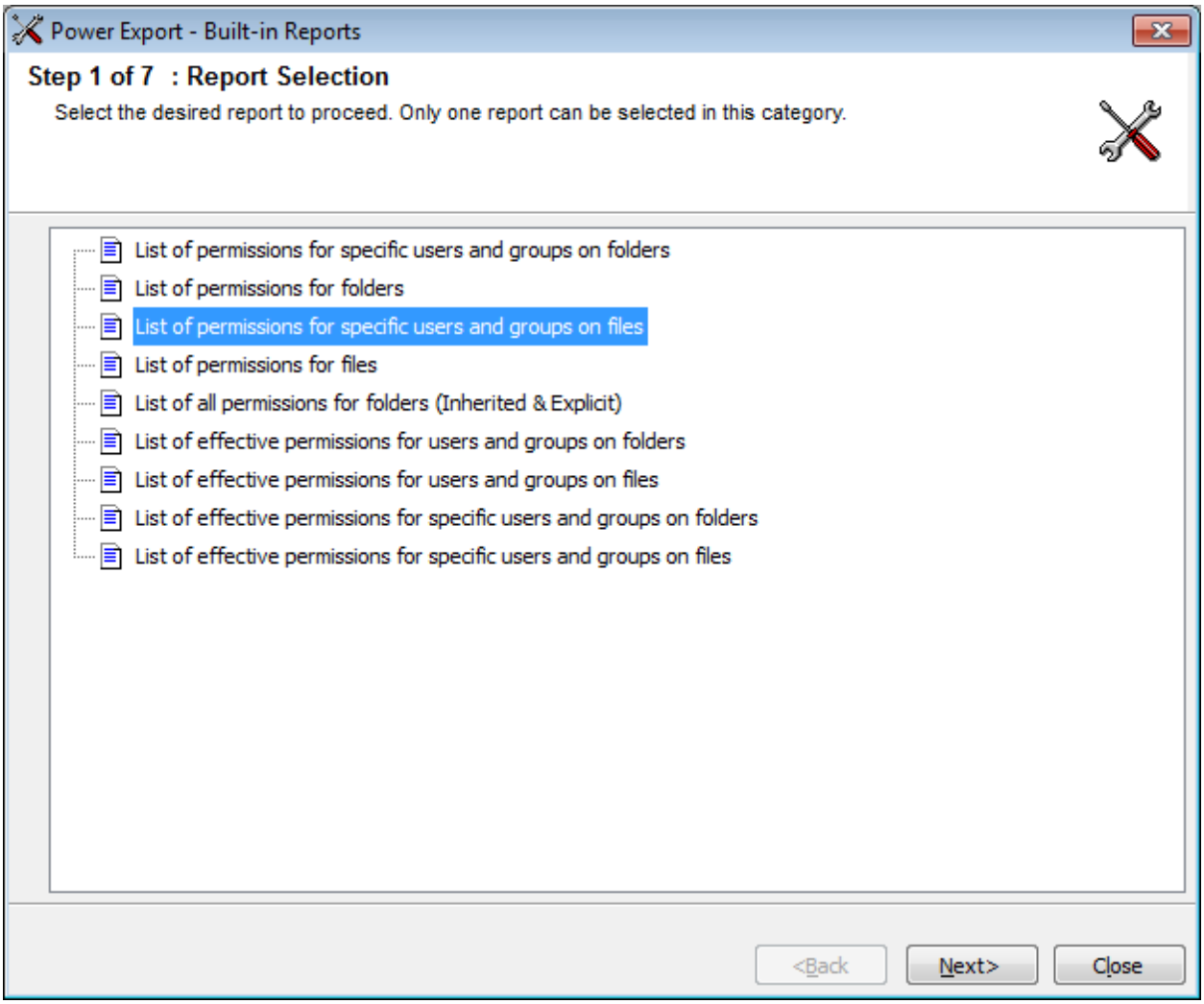
List of permissions for specific users and groups on files

This report allows you to view file permissions for specific users and groups.

Select

option under Power Export. This will bring up the Power Export Wizard.

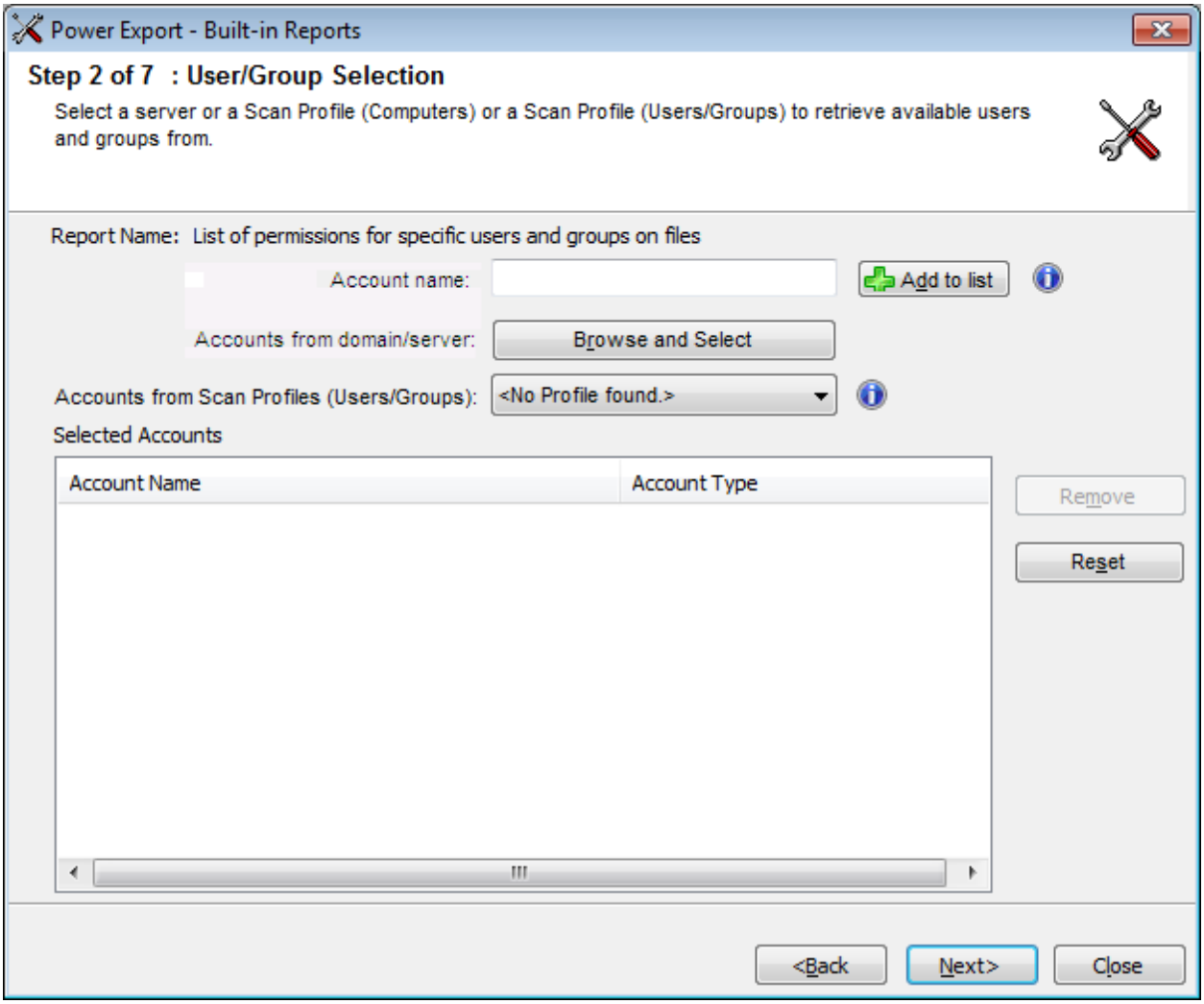
Step 1: Report Selection

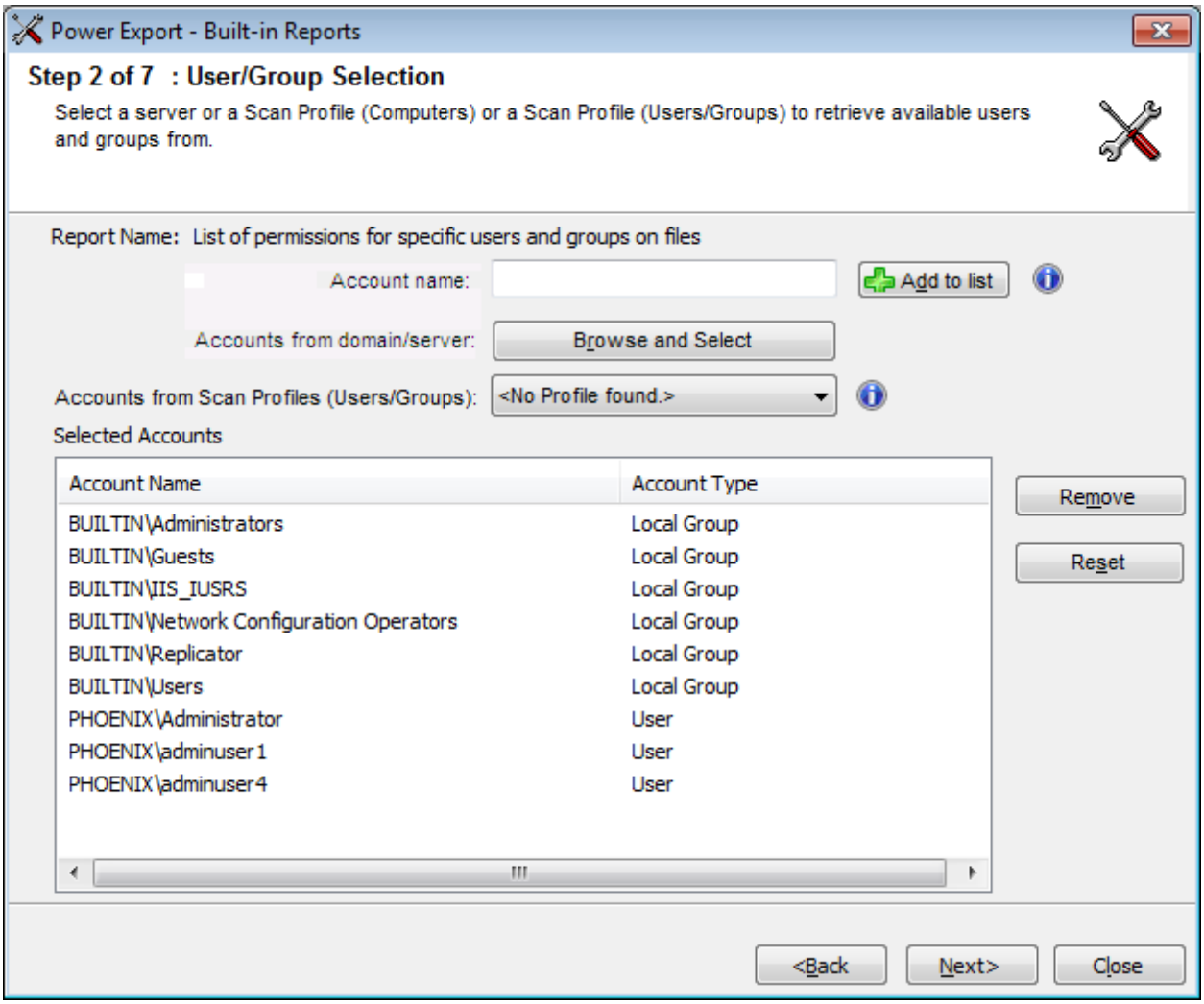

Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.

3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: User and/or Group Selection

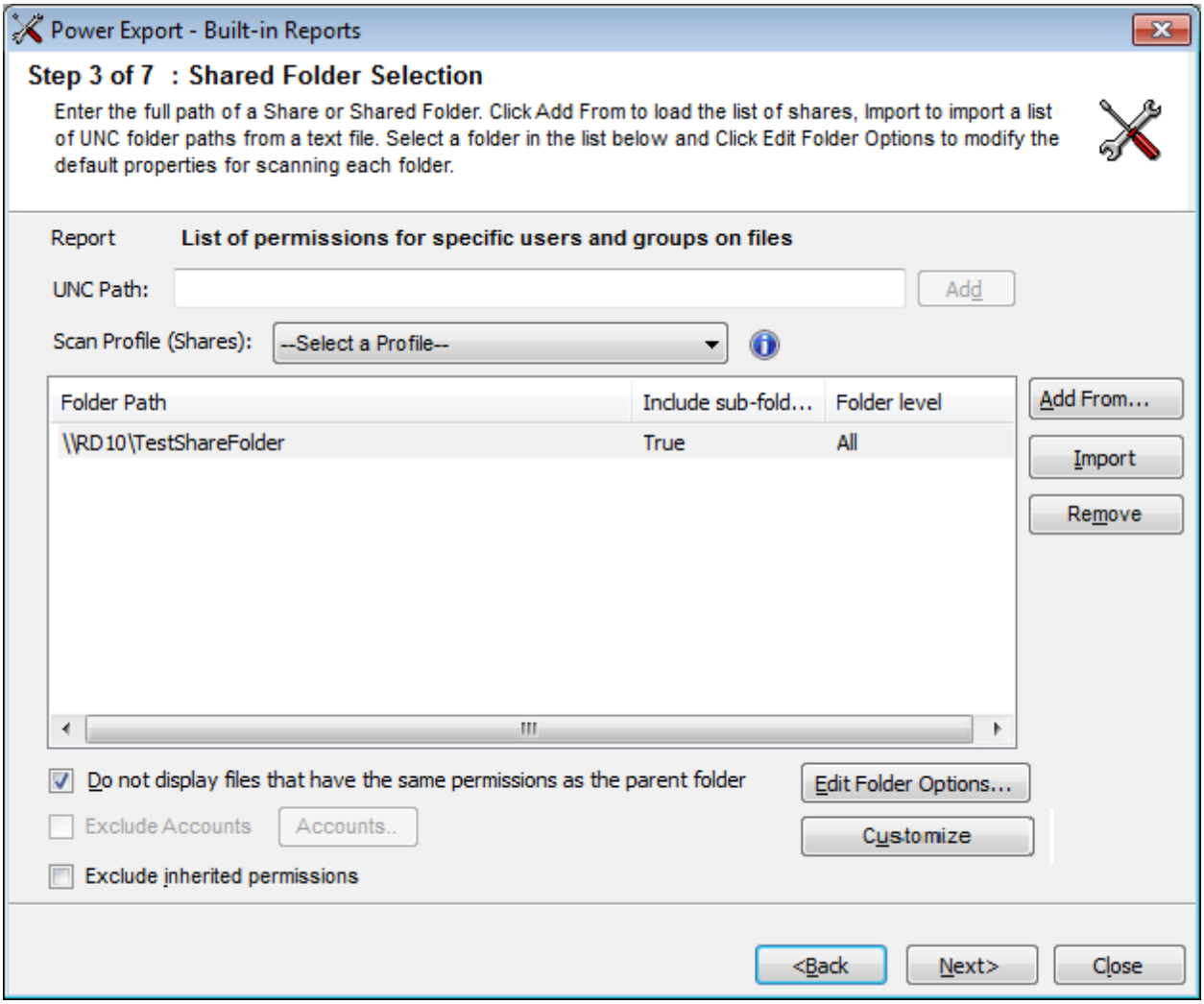

Power Export - Built-in Reports
Step 2 of 7 : User/Group Selection
Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.
Report Name: List of permissions for specific users and groups on files
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
<No Profile found.>
Selected Accounts
Account Name
Account Type
Remove
Reset
<Back
Next>
Close



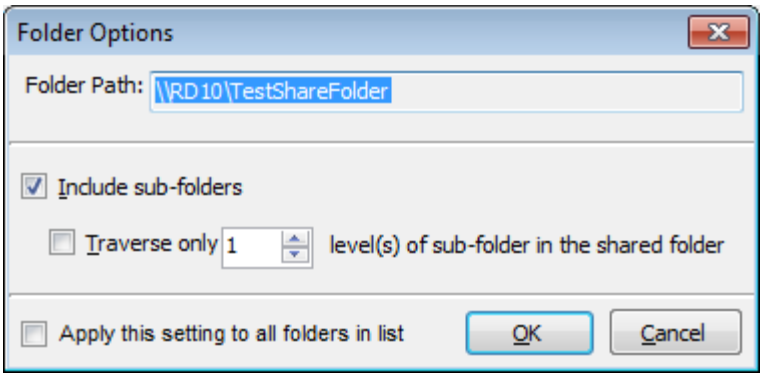
- Use Select a Scan Profile (Users/Groups) option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

1. Select the user or group, for which you wish to run the permissions report.
2. The selected users will be added to the wizard as shown above:
3. Click Next to proceed to the Next step.

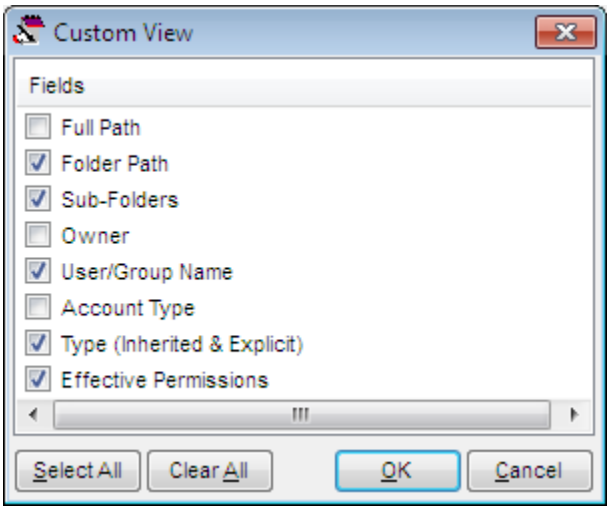
Step 3: Shared Folder Selection


Power Export - Built-in Reports
Step 3 of 7 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of permissions for specific users and groups on files
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display files that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
Exclude inherited permissions
<Back
Next>
Close

1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Files that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want files with identical permissions as the parent folder reported, then select **Do not display files that have same permissions as the parent folder option**. This option will not report files with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:

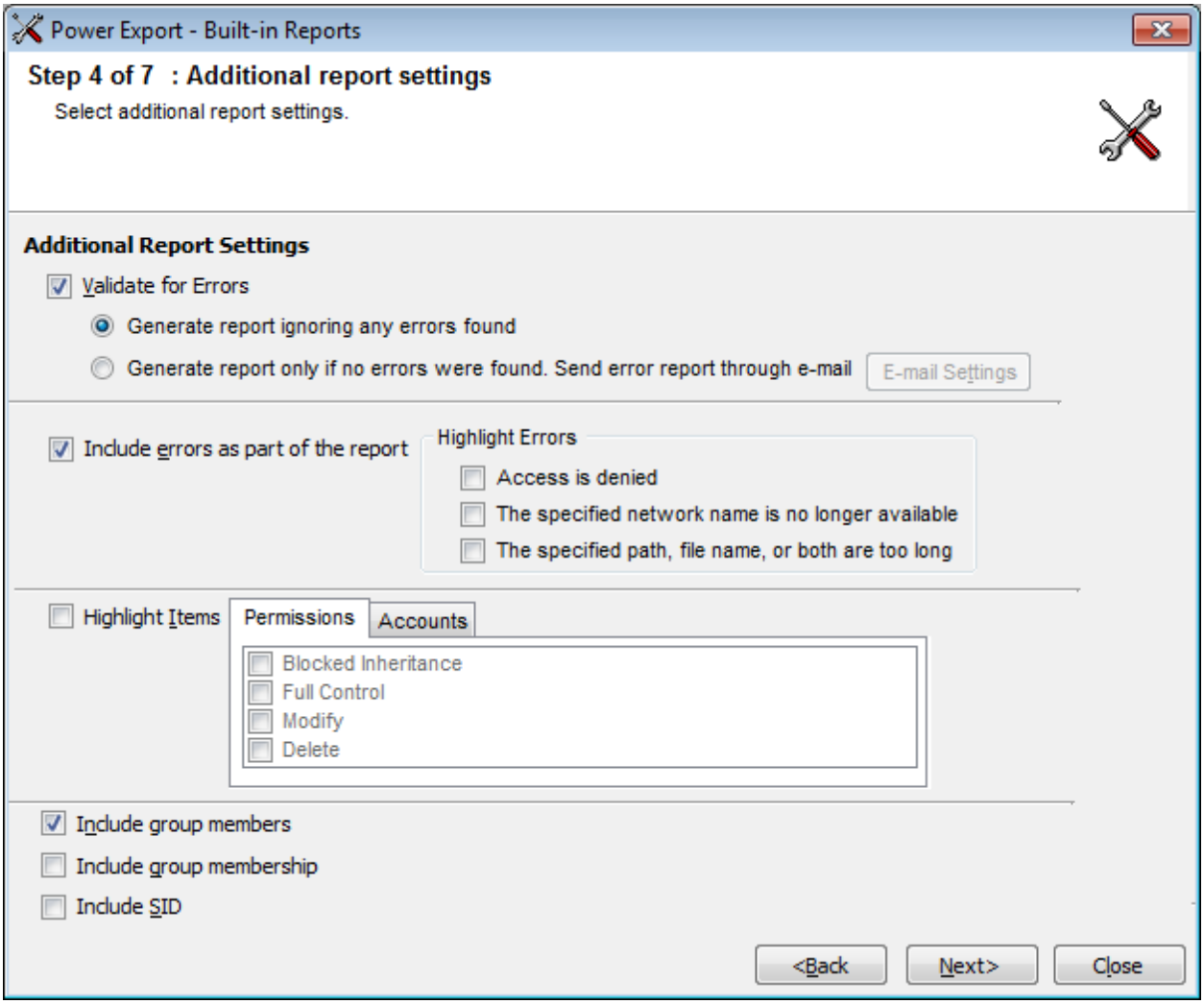


5. Modify the folder options as required and click **OK**.
6. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



7. Select the customize options as required and click **OK**.
8. You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.
9. Click **Next** to proceed to the Next step.

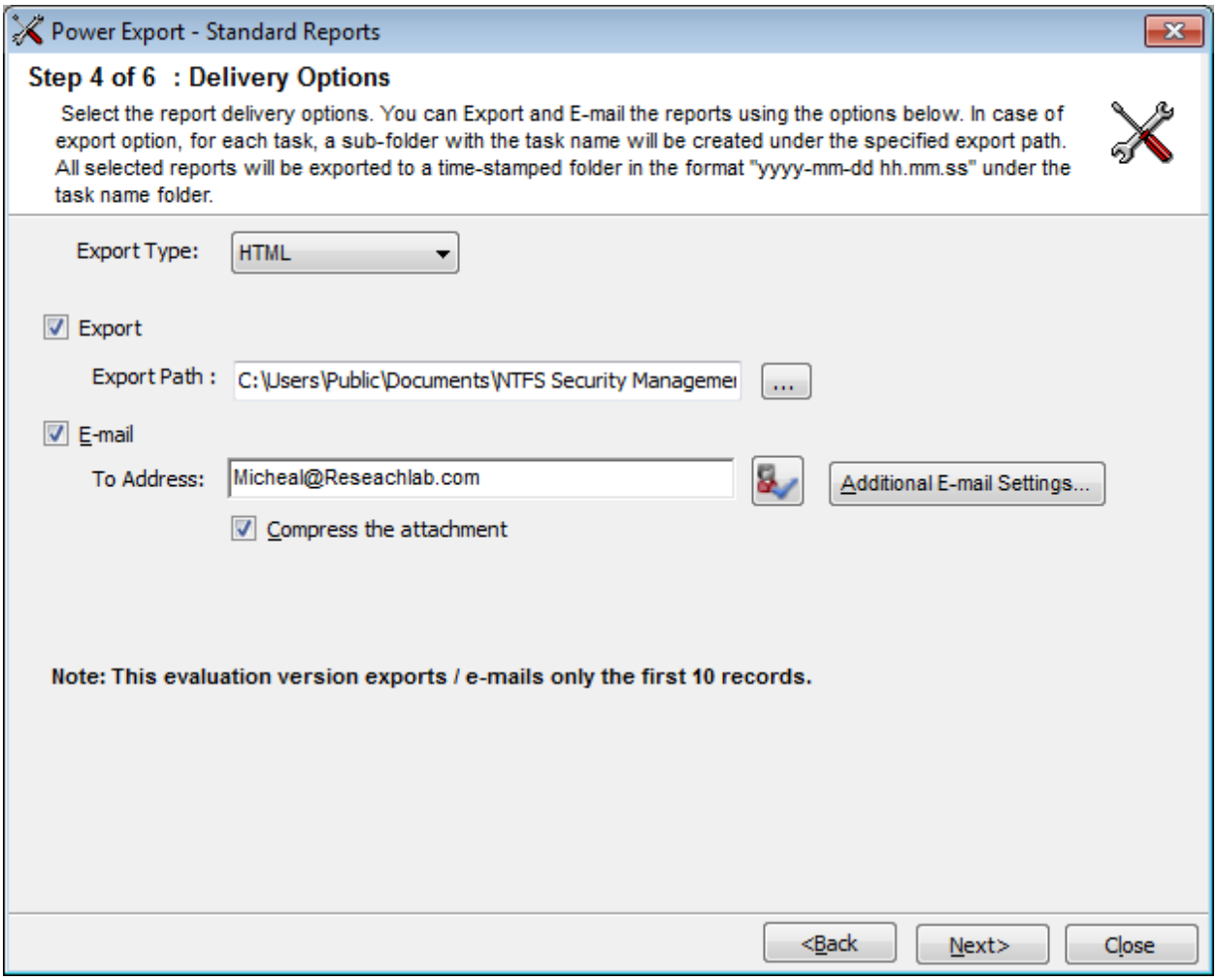
Step 4: Additional report settings



1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

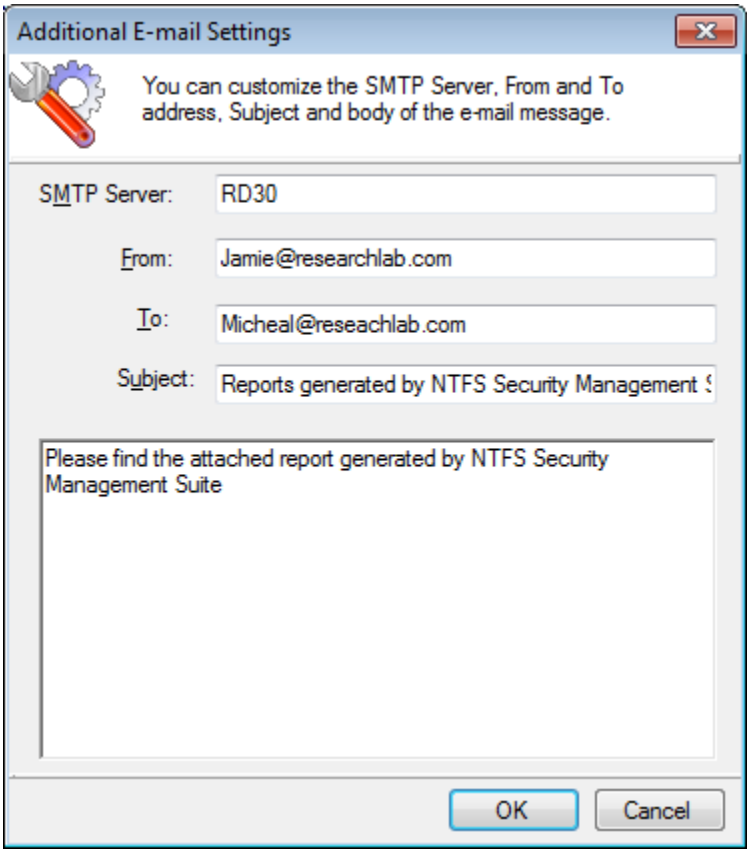
4. You may also select **Include group members** for include members of a group and their sub-group members at all group levels in the report.
5. You may also select **Include group membership** for include membership information of user and group in the report.
6. You may also select **Include SID** for include SID value for user in the report.
7. Click Next to proceed to the Next step.

Step 4: Delivery Options

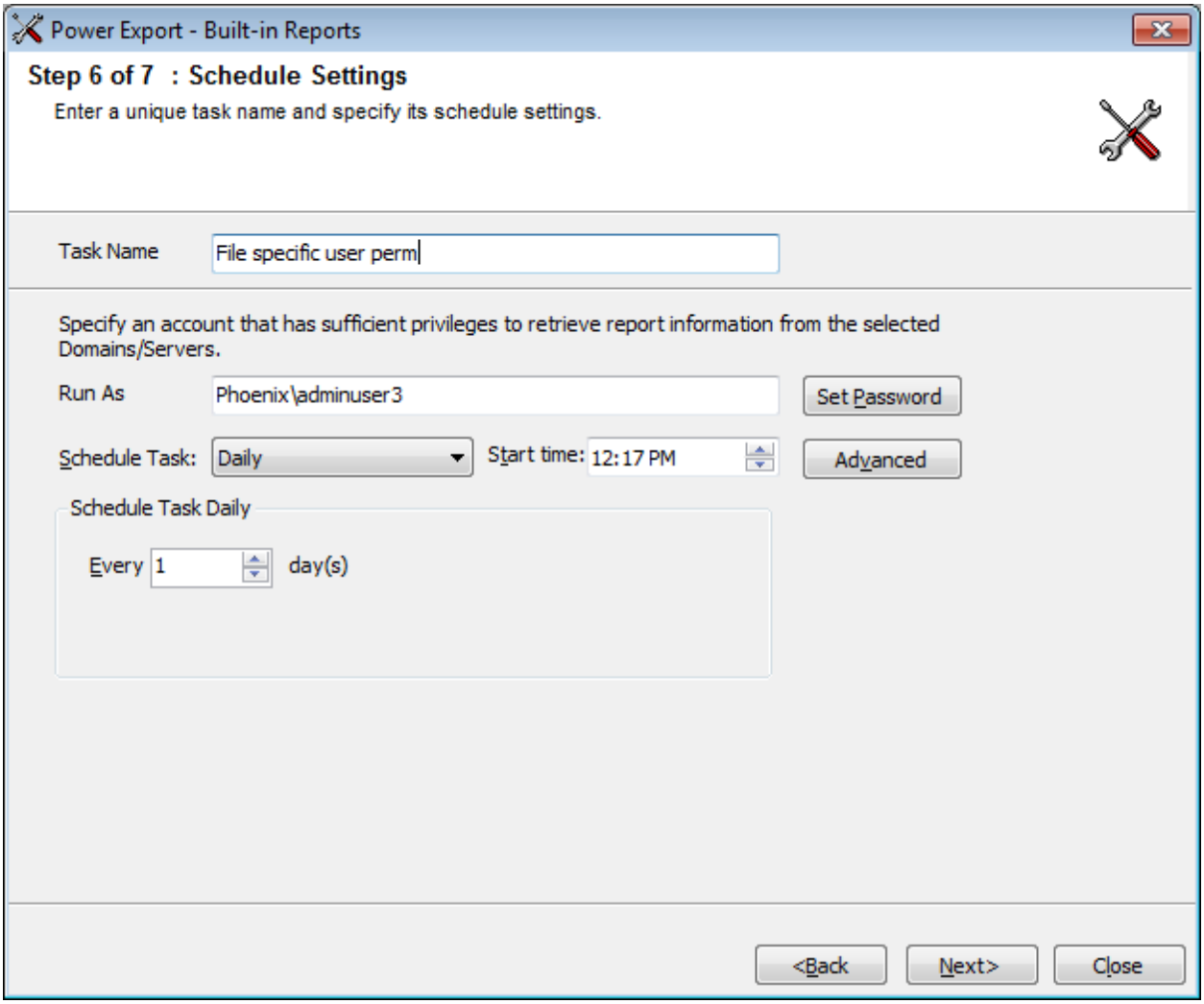

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

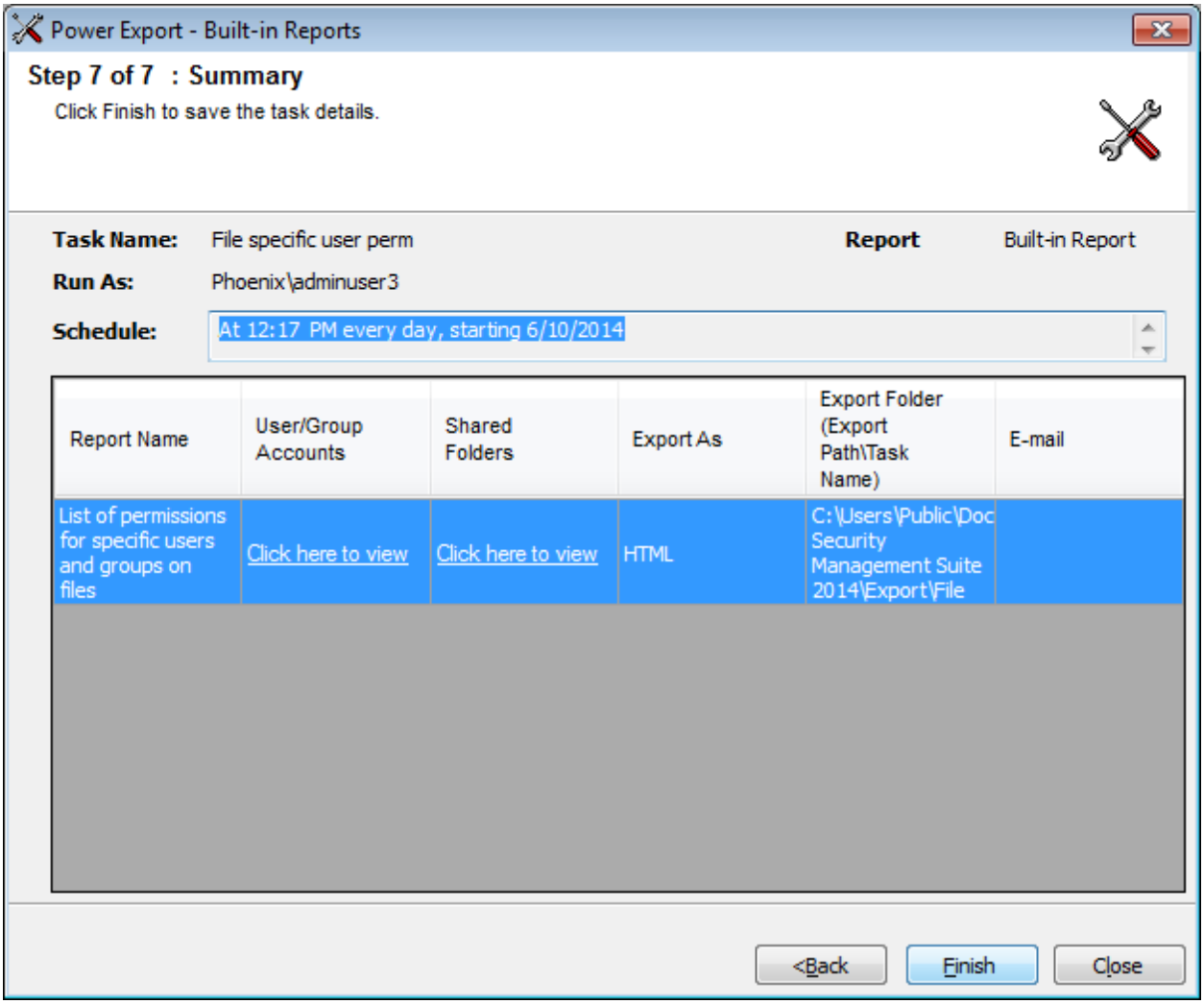

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Scheduled Tasks folder.

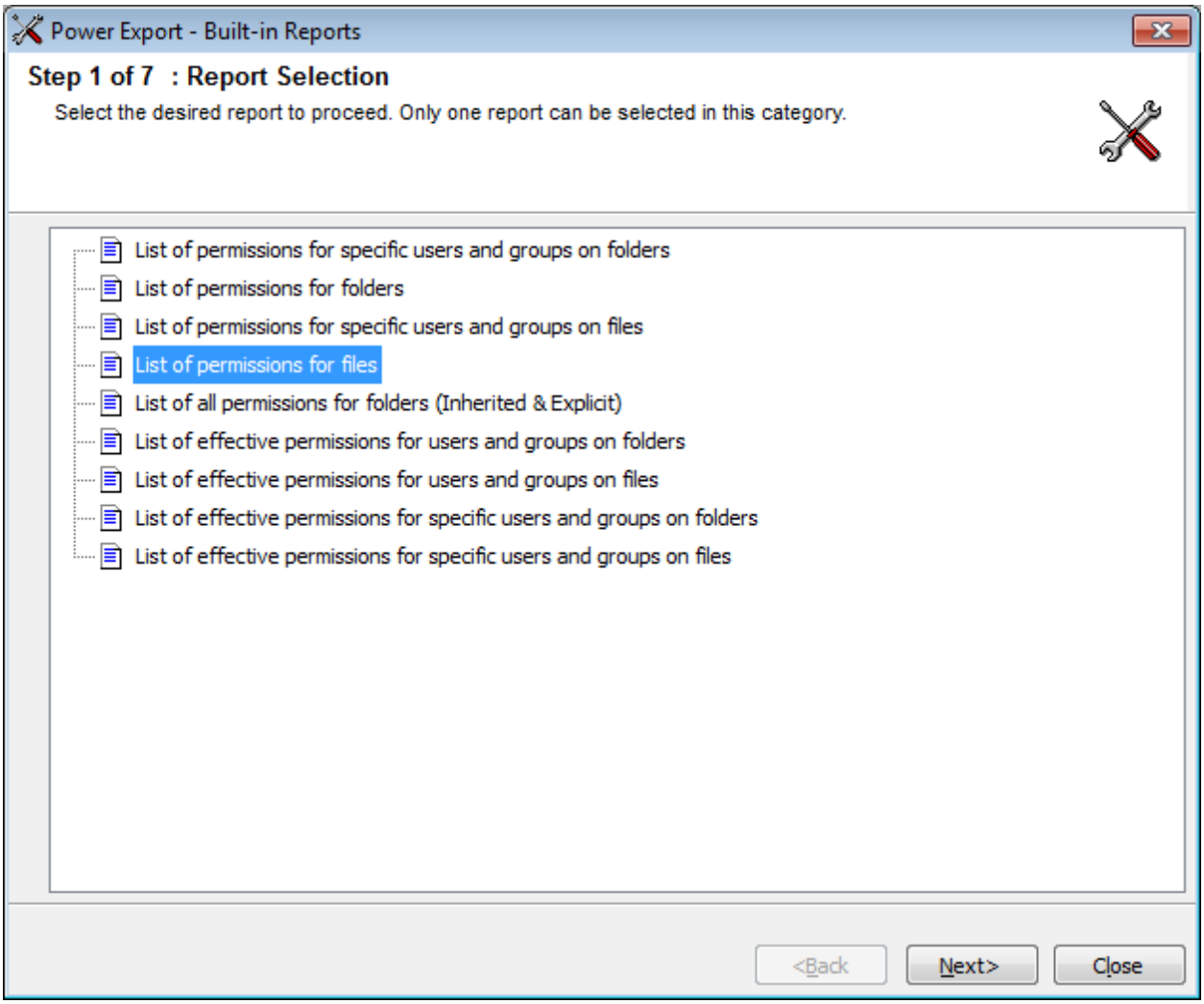
List of permissions for files

This report allows you to view the associated file permissions under a specific set of folders.

Select

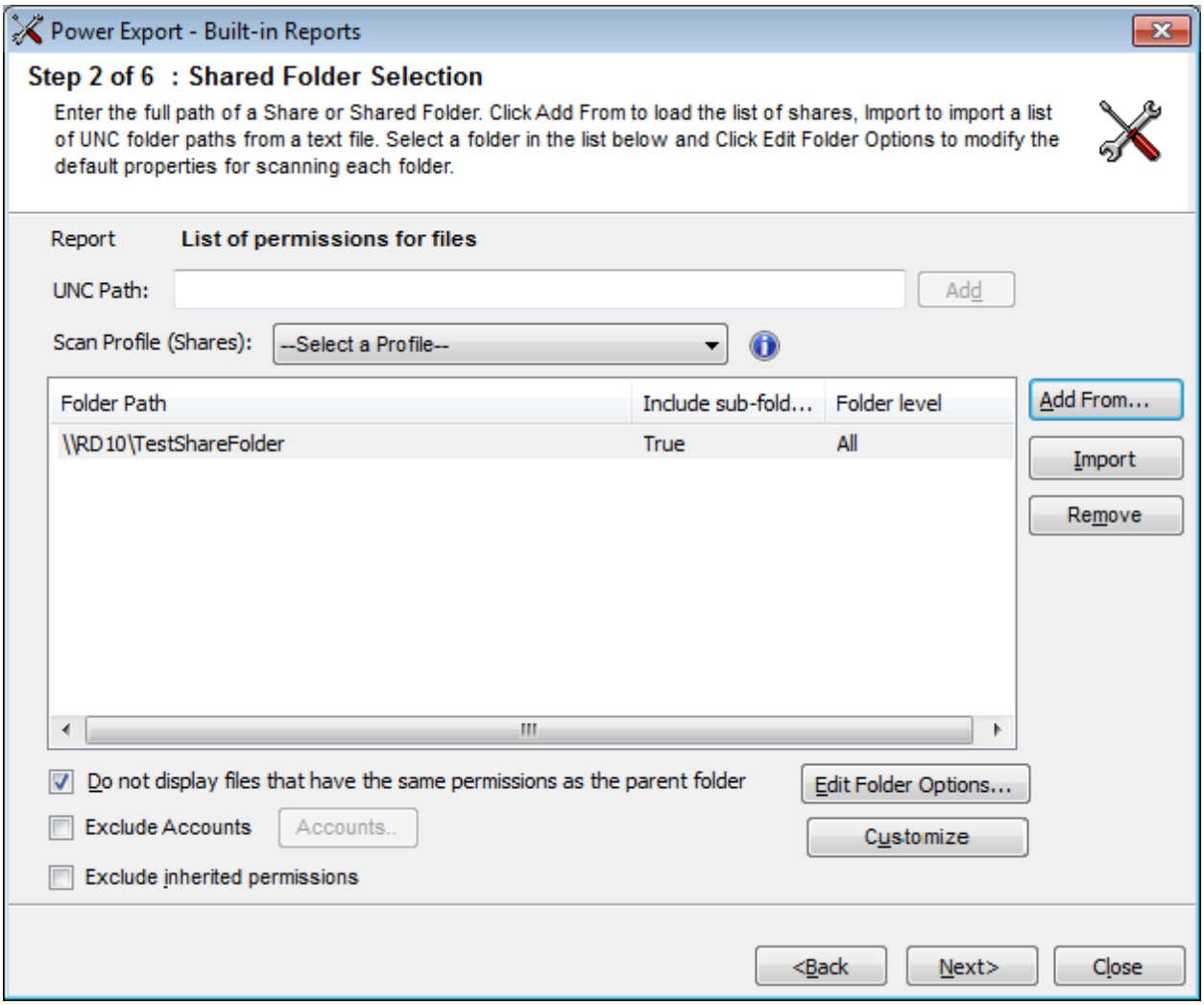
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection

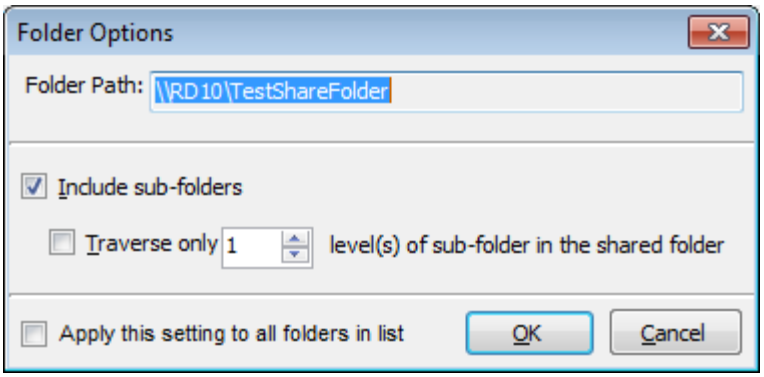

Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

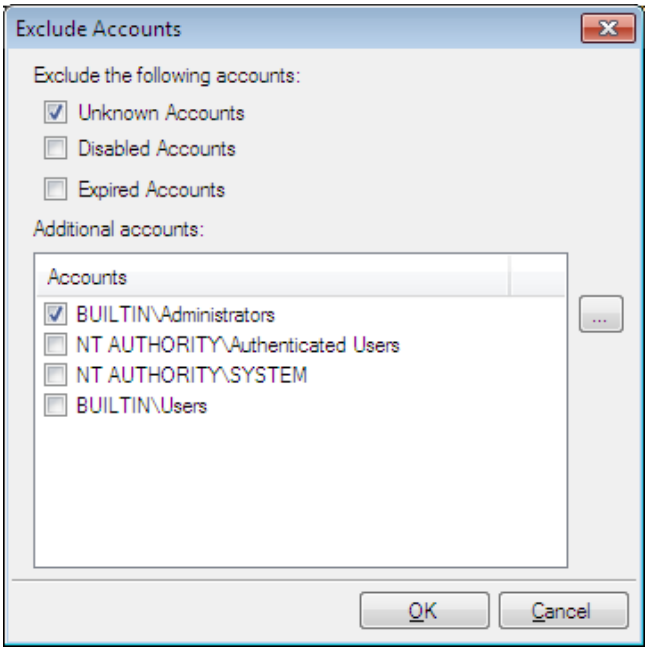
Step 2: Shared Folder Selection


Power Export - Built-in Reports
Step 2 of 6 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of permissions for files
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display files that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
Exclude inherited permissions
<Back
Next>
Close

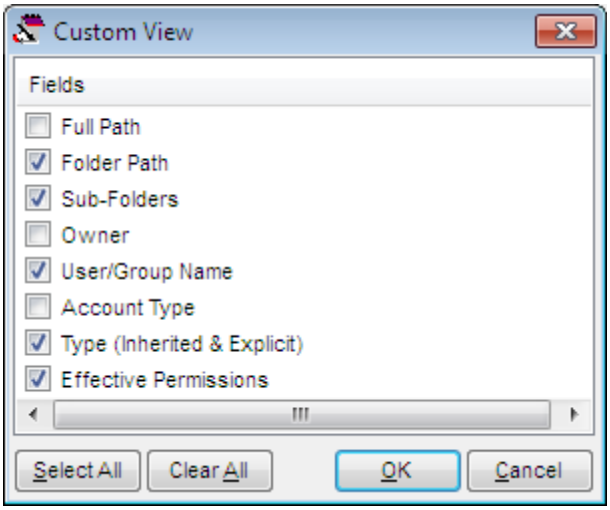
1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Files that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want files with identical permissions as the parent folder reported, then select **Do not display files that have same permissions as the parent folder option**. This option will not report files with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



5. Modify the folder options as required and click **OK**.
6. If you want to exclude specific accounts select **Exclude Accounts** option. Click **Accounts...** button. That will show up a window as shown below:

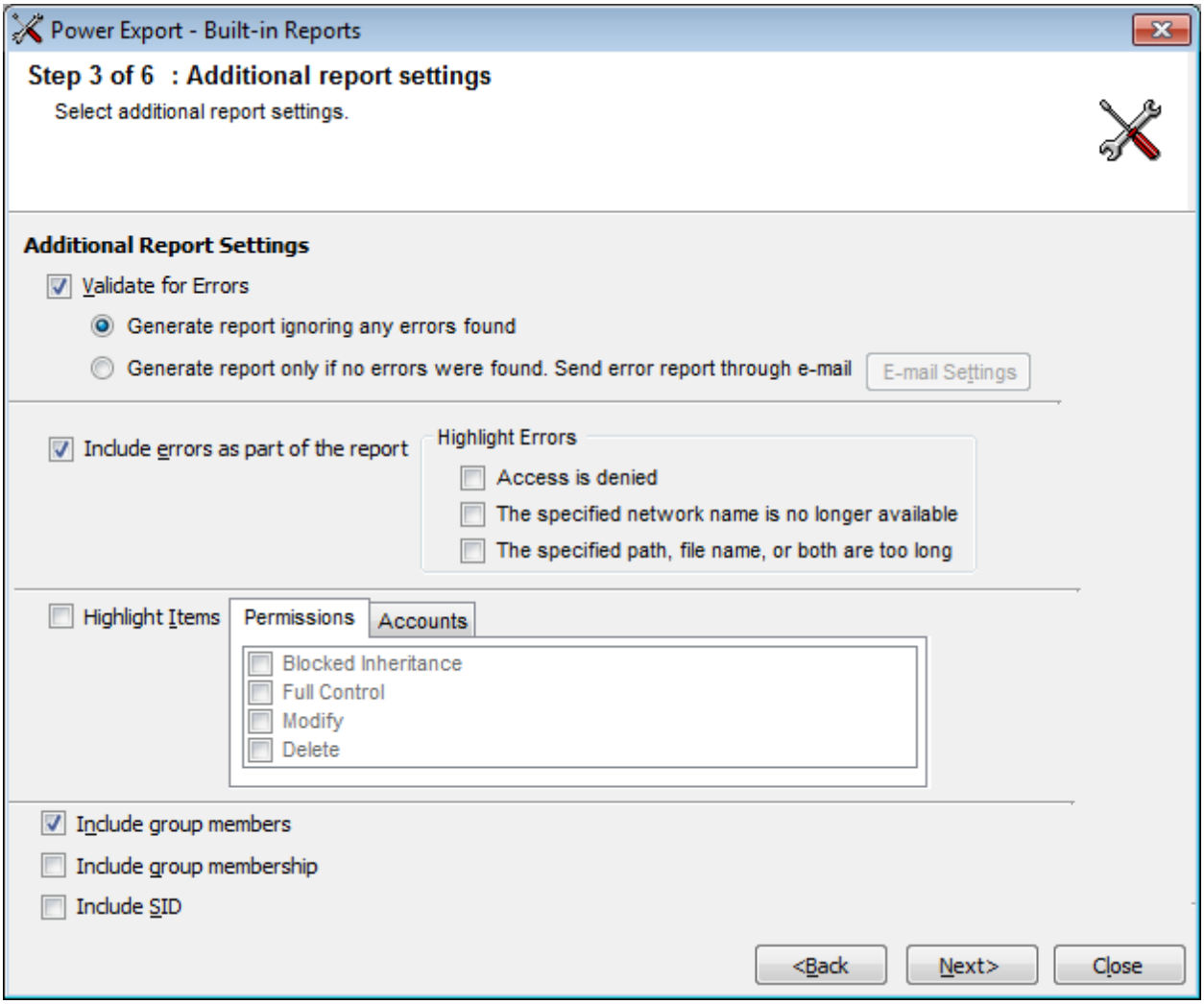


7. Select the accounts for which you want to exclude and click **OK**.
8. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



9. Select the customize options as required and click **OK**.
10. You can select **Exclude inherited permissions** option to exclude inherited permissions from the report.
11. Click **Next** to proceed to the Next step.

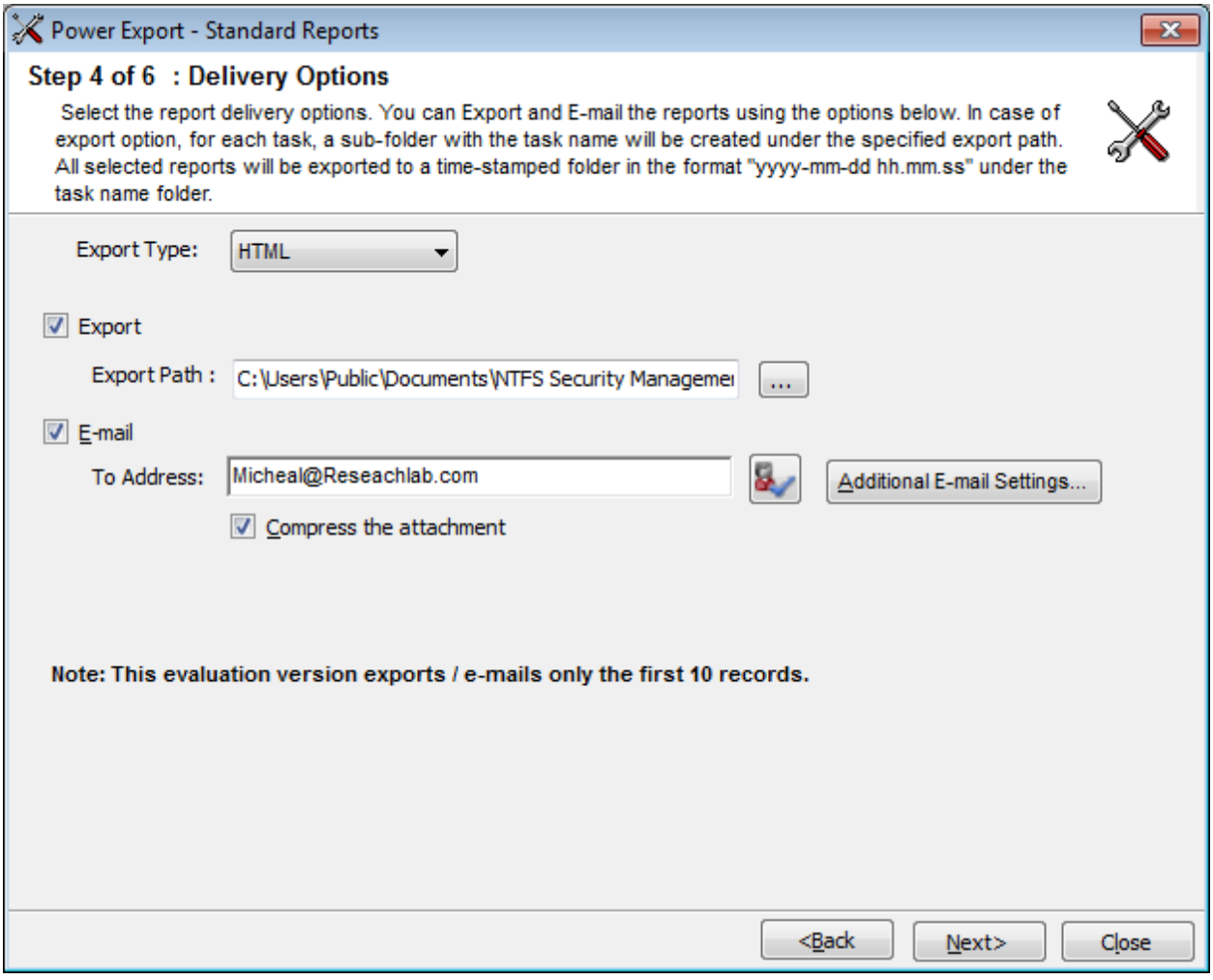
Step 3: Additional report settings



1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

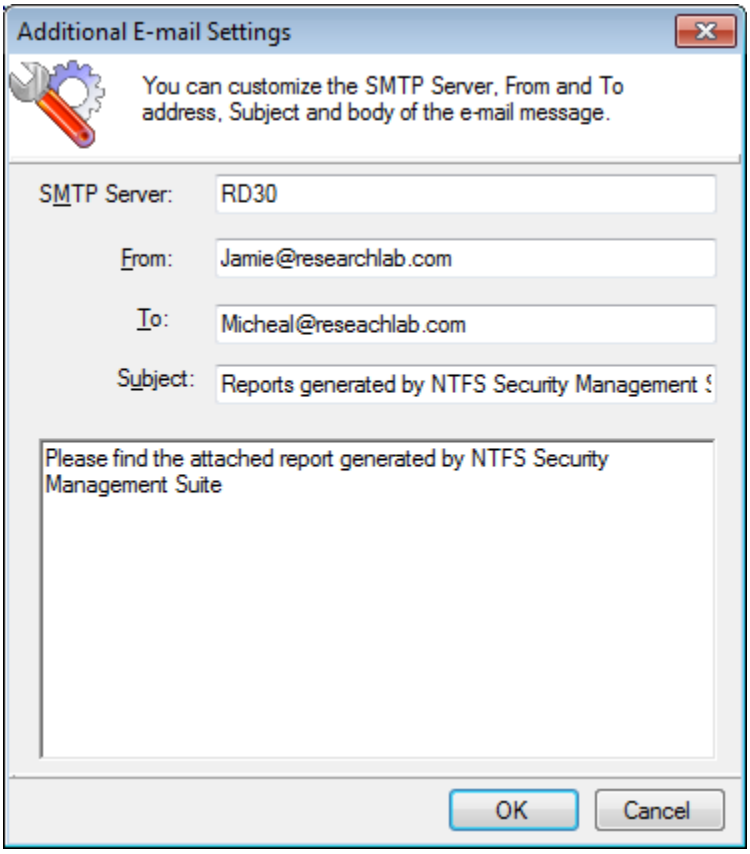
4. You may also select **Include group members** for include members of a group and their sub-group members at all group levels in the report.
5. You may also select **Include group membership** for include membership information of user and group in the report.
6. You may also select **Include SID** for include SID value for user in the report.
7. Click **Next** to proceed to the Next step.

Step 4: Delivery Options

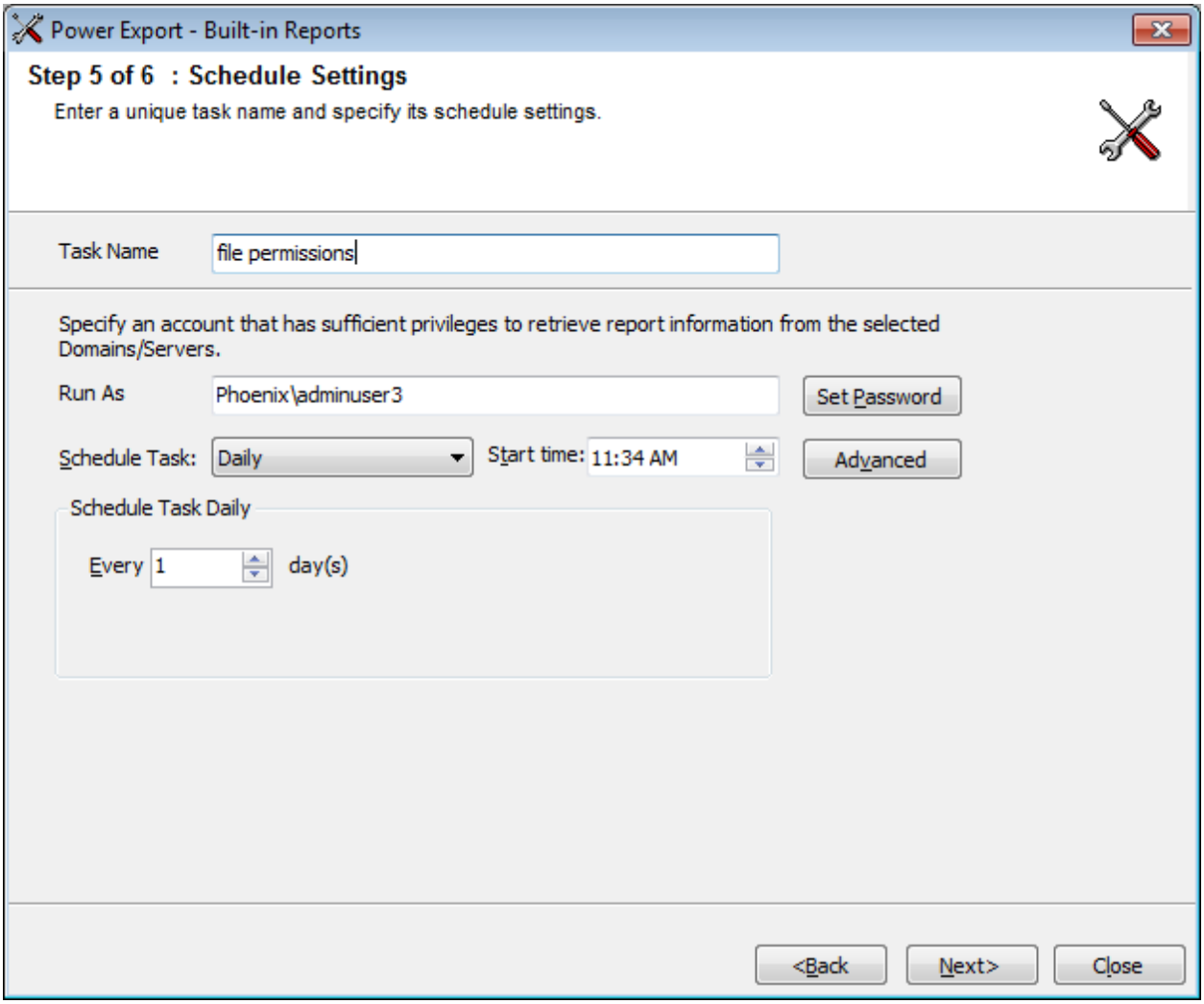

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

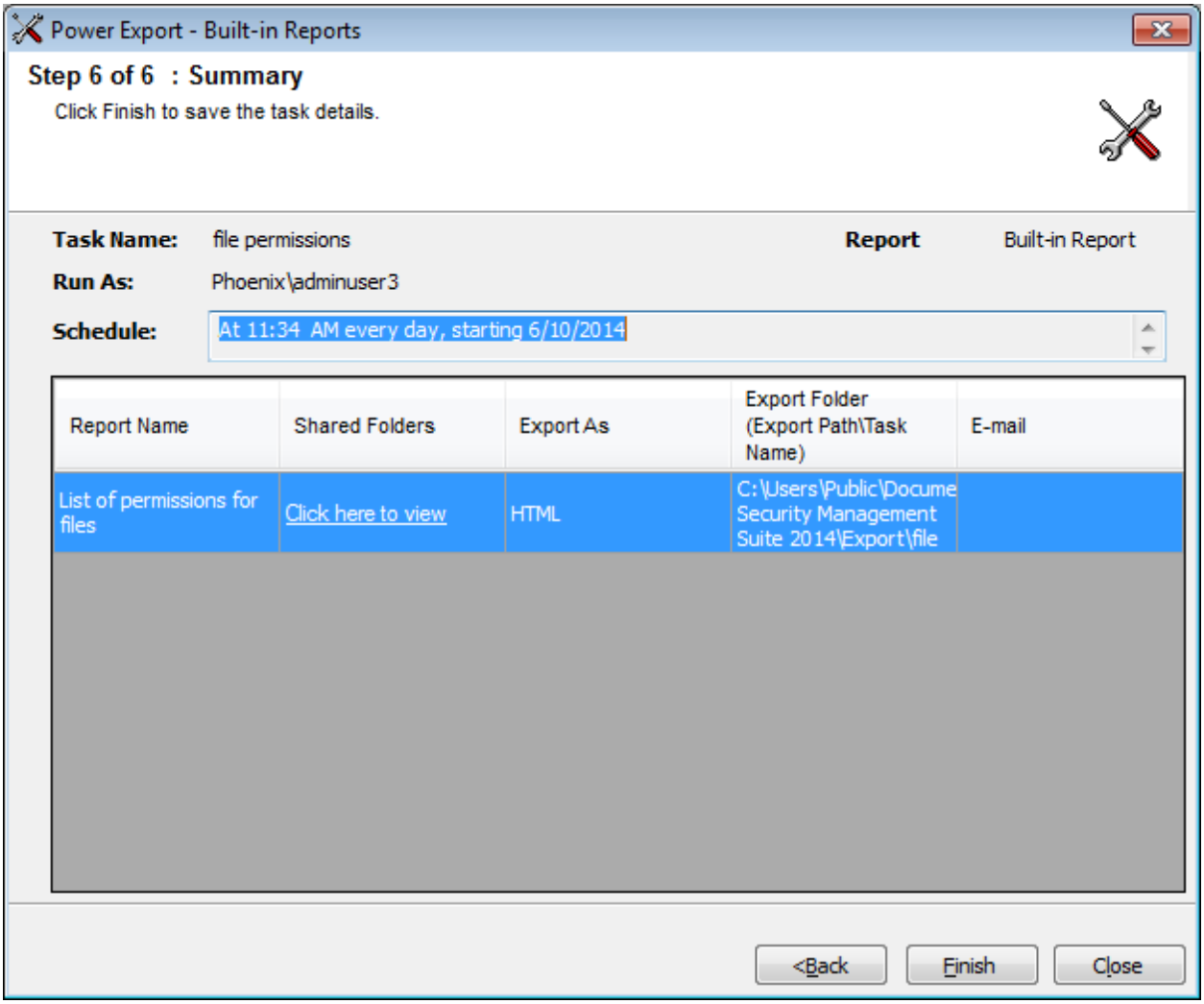


Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Scheduled Tasks folder.

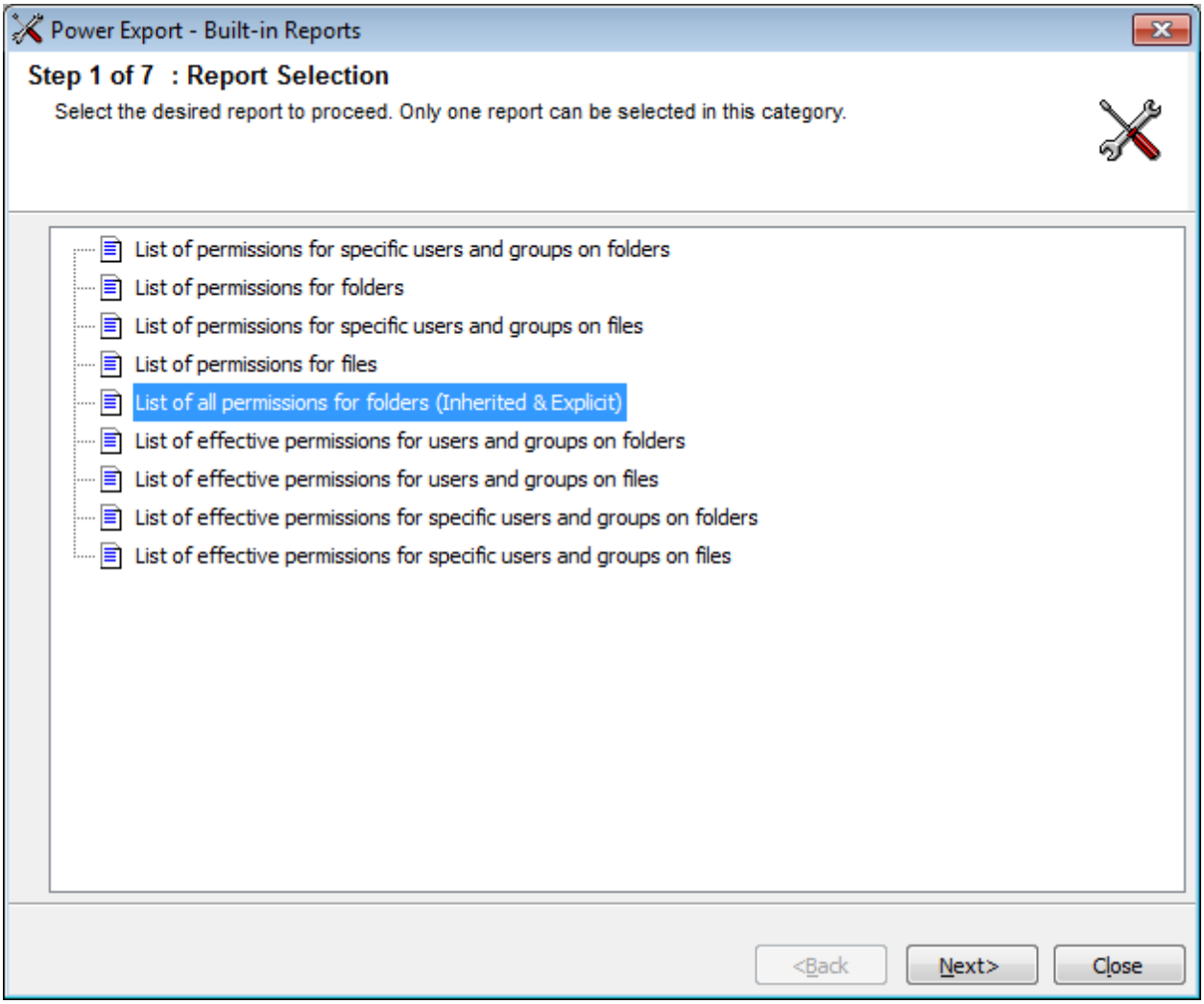
List of all permissions for folders (Inherited & Explicit)

This report lists the permissions (explicit and inherit) assigned to the users for a set of folders.

Select

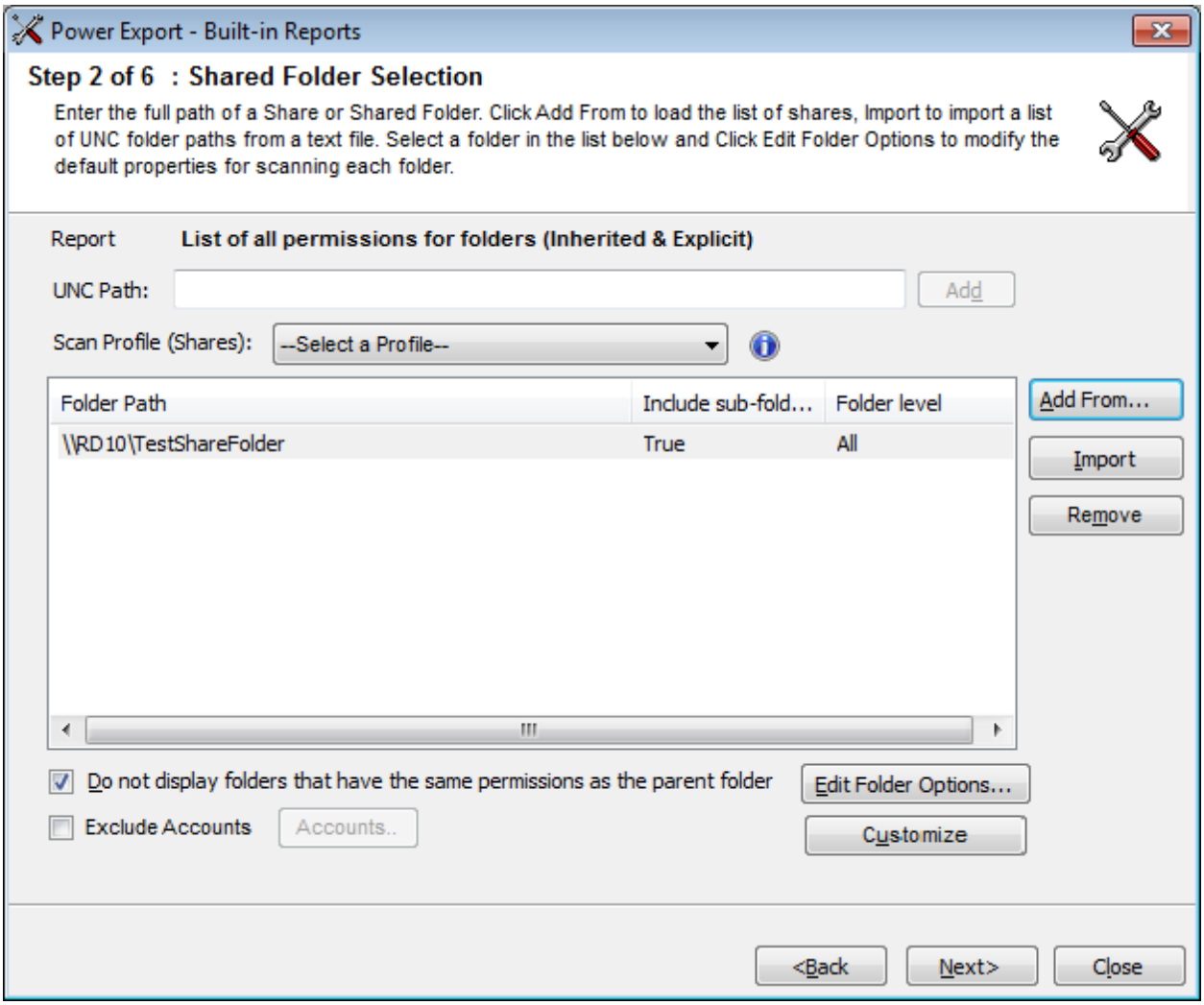
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection


Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

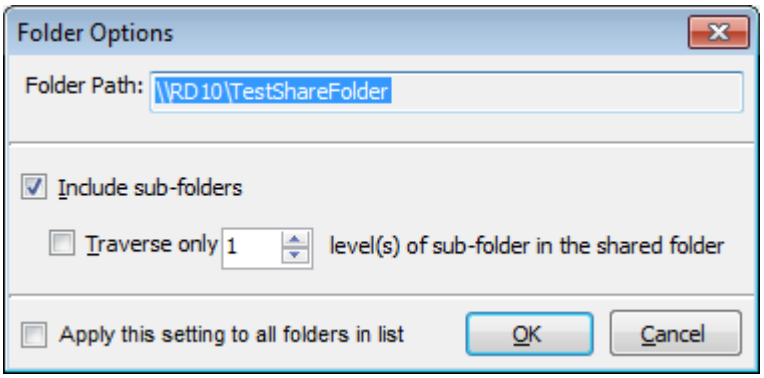
1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: Shared Folder Selection

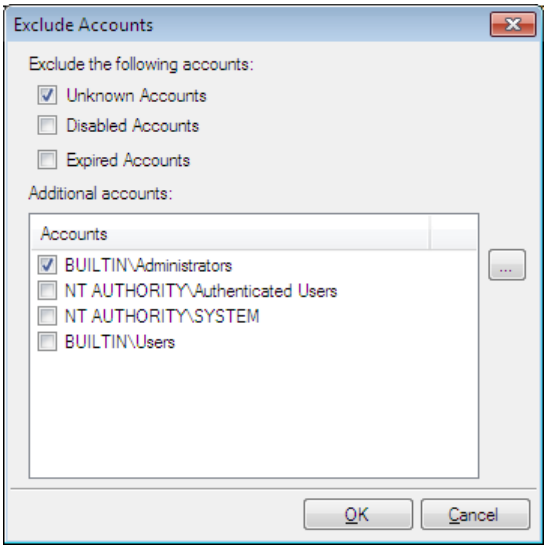

Power Export - Built-in Reports
Step 2 of 6 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of all permissions for folders (Inherited & Explicit)
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
<Back
Next>
Close

1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

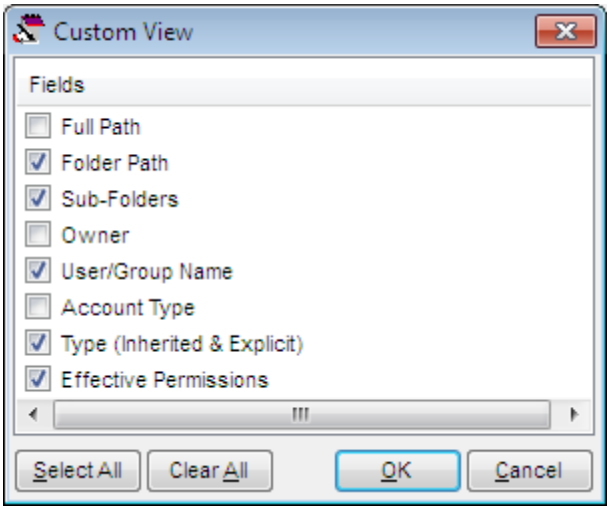
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



5. Modify the folder options as required and click **OK**.
6. If you want to exclude specific accounts select **Exclude Accounts** option. Click **Accounts...** button. That will show up a window as shown below:

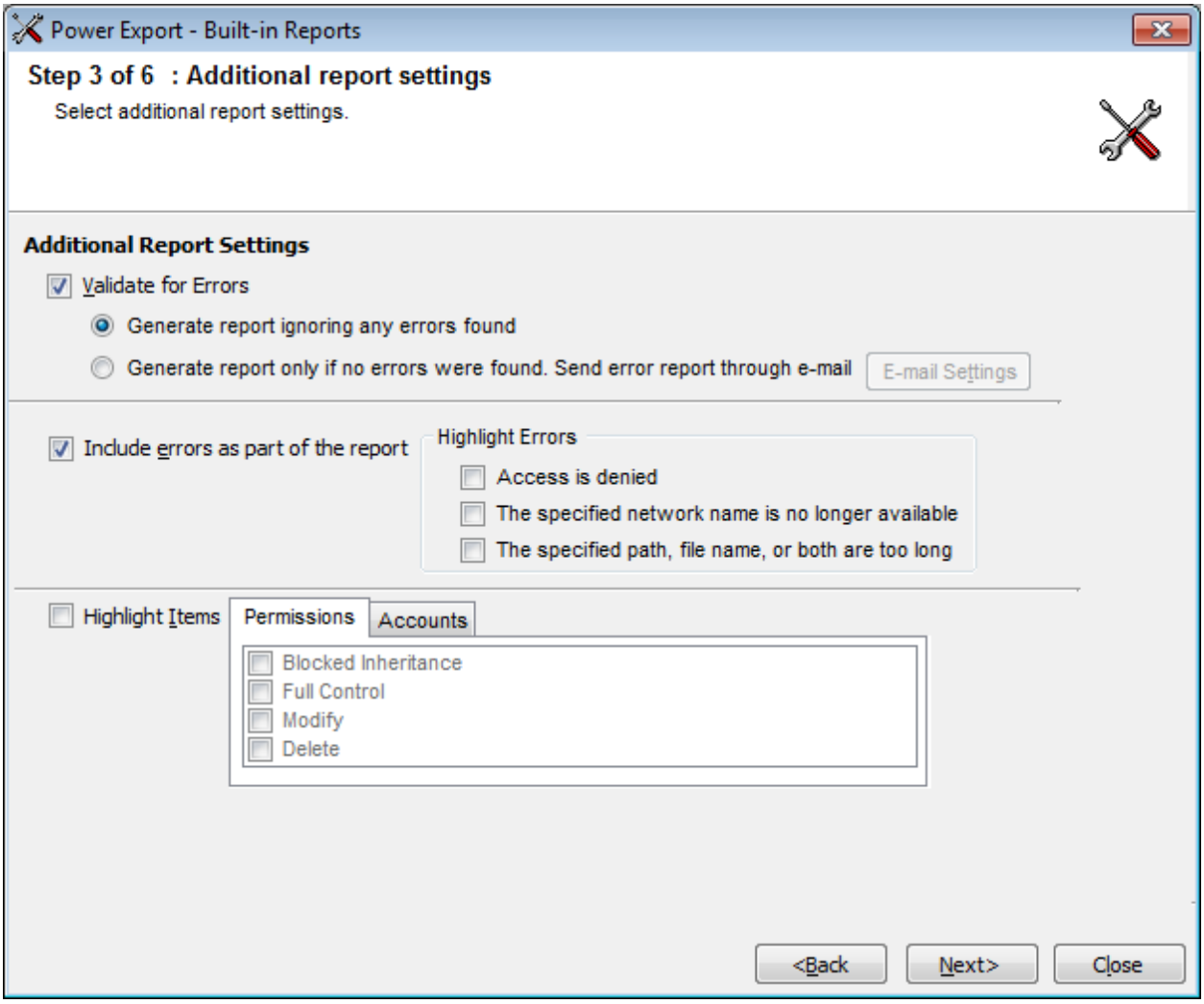


7. Select the accounts for which you want to exclude and click **OK**.
8. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



9. Select the customize options as required and click **OK**.
10. Click **Next** to proceed to the Next step.

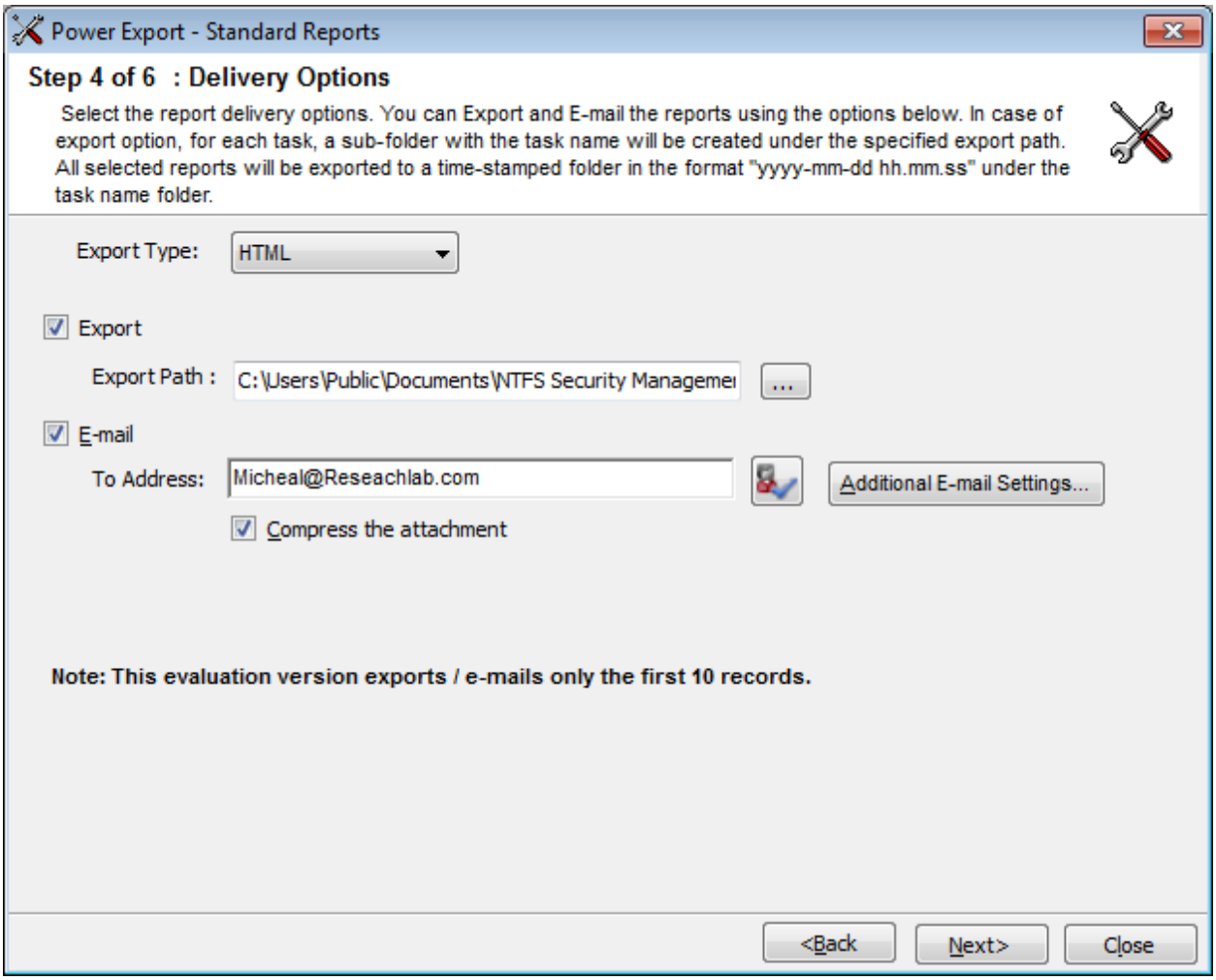
Step 3: Additional report settings


Power Export - Built-in Reports
Step 3 of 6 : Additional report settings
Select additional report settings.
Additional Report Settings
Validate for Errors
Generate report ignoring any errors found
Generate report only if no errors were found. Send error report through e-mail
E-mail Settings
Include errors as part of the report
Highlight Errors
Access is denied
The specified network name is no longer available
The specified path, file name, or both are too long
Highlight Items
Permissions
Accounts
Blocked Inheritance
Full Control
Modify
Delete
<Back
Next>
Close

1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Selecting error information that needs to be highlighted.

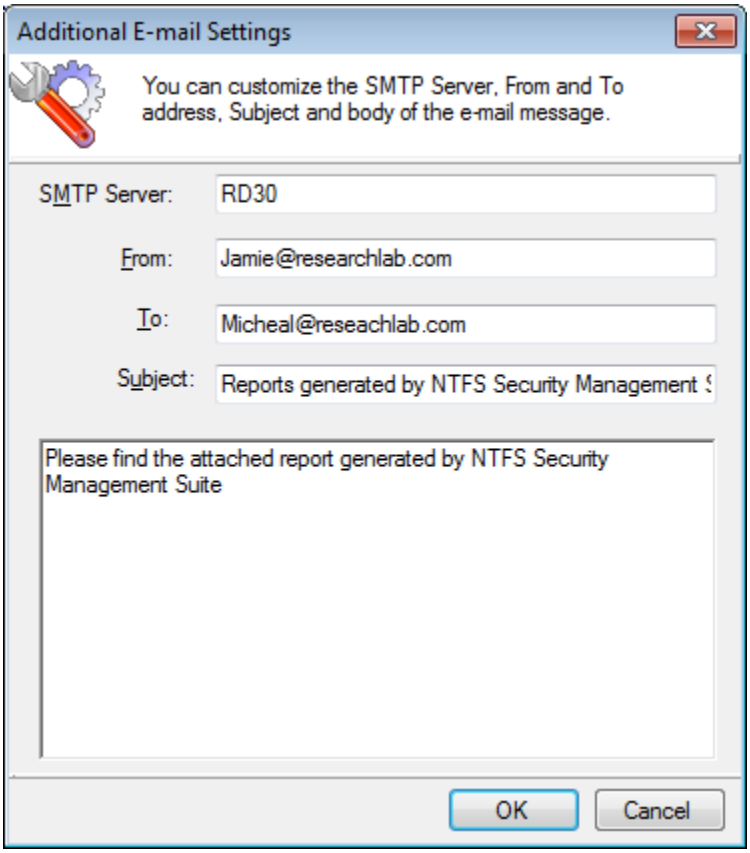
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.
4. Click **Next** to proceed to the Next step.

Step 4: Delivery Options

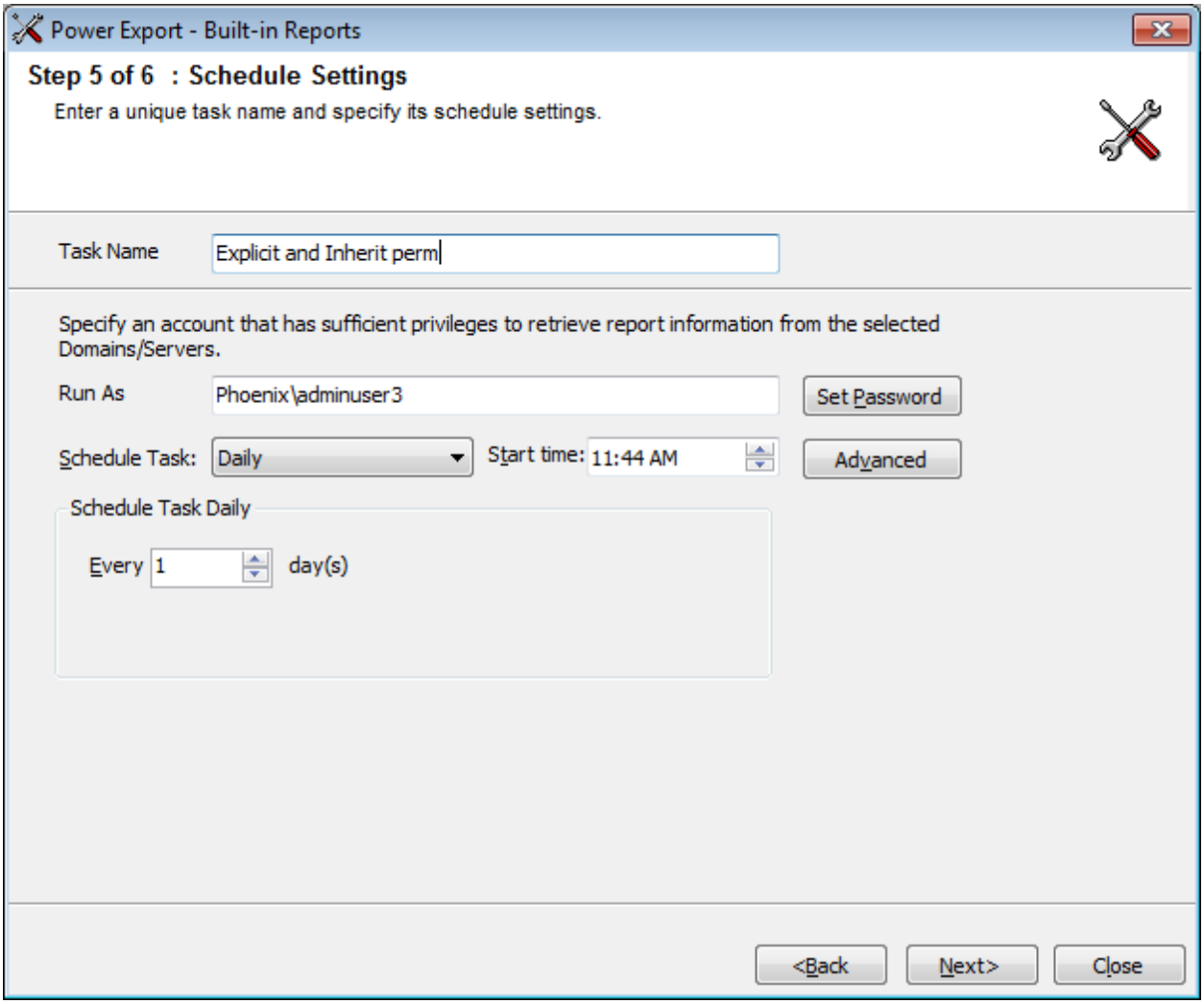

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

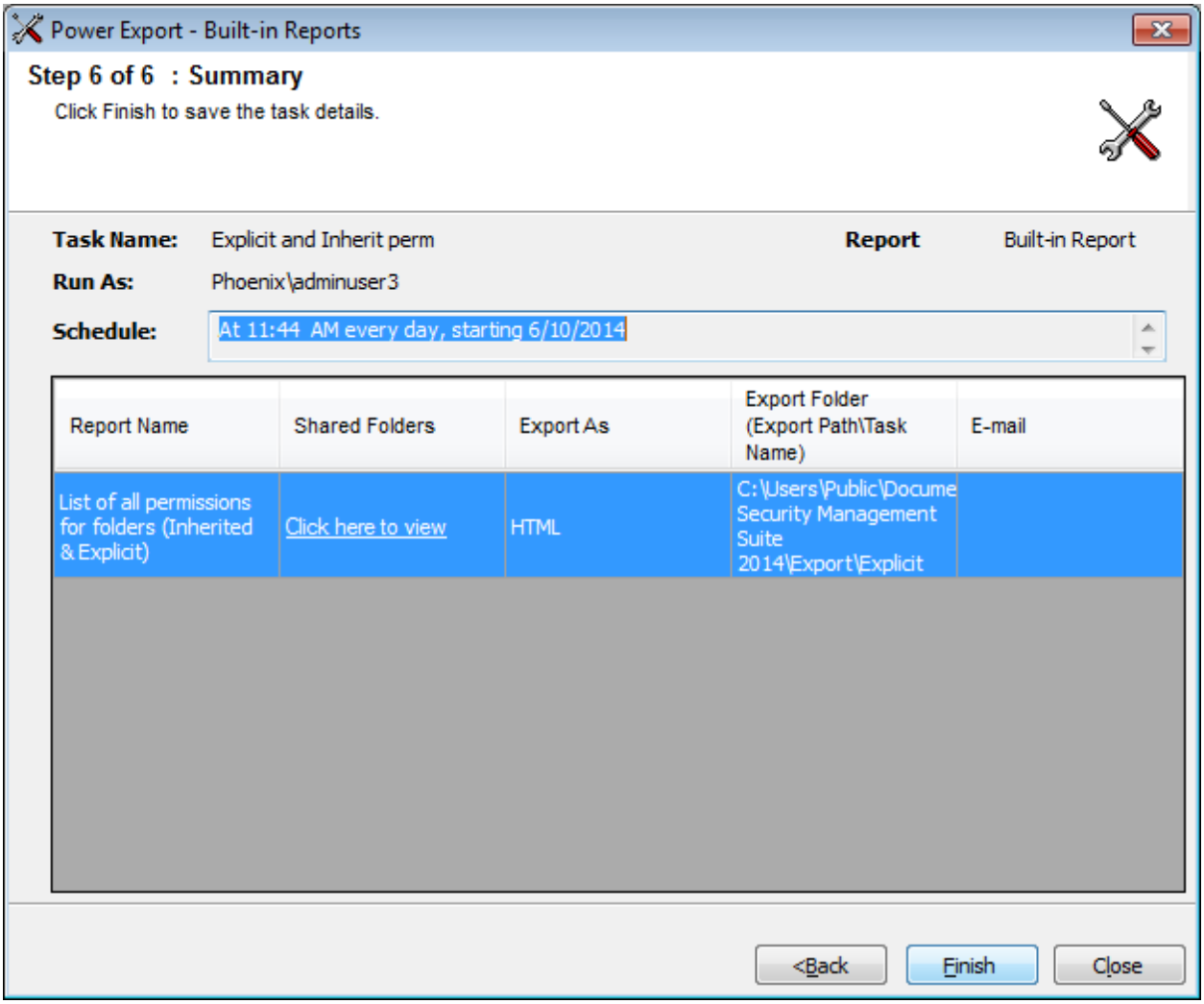

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

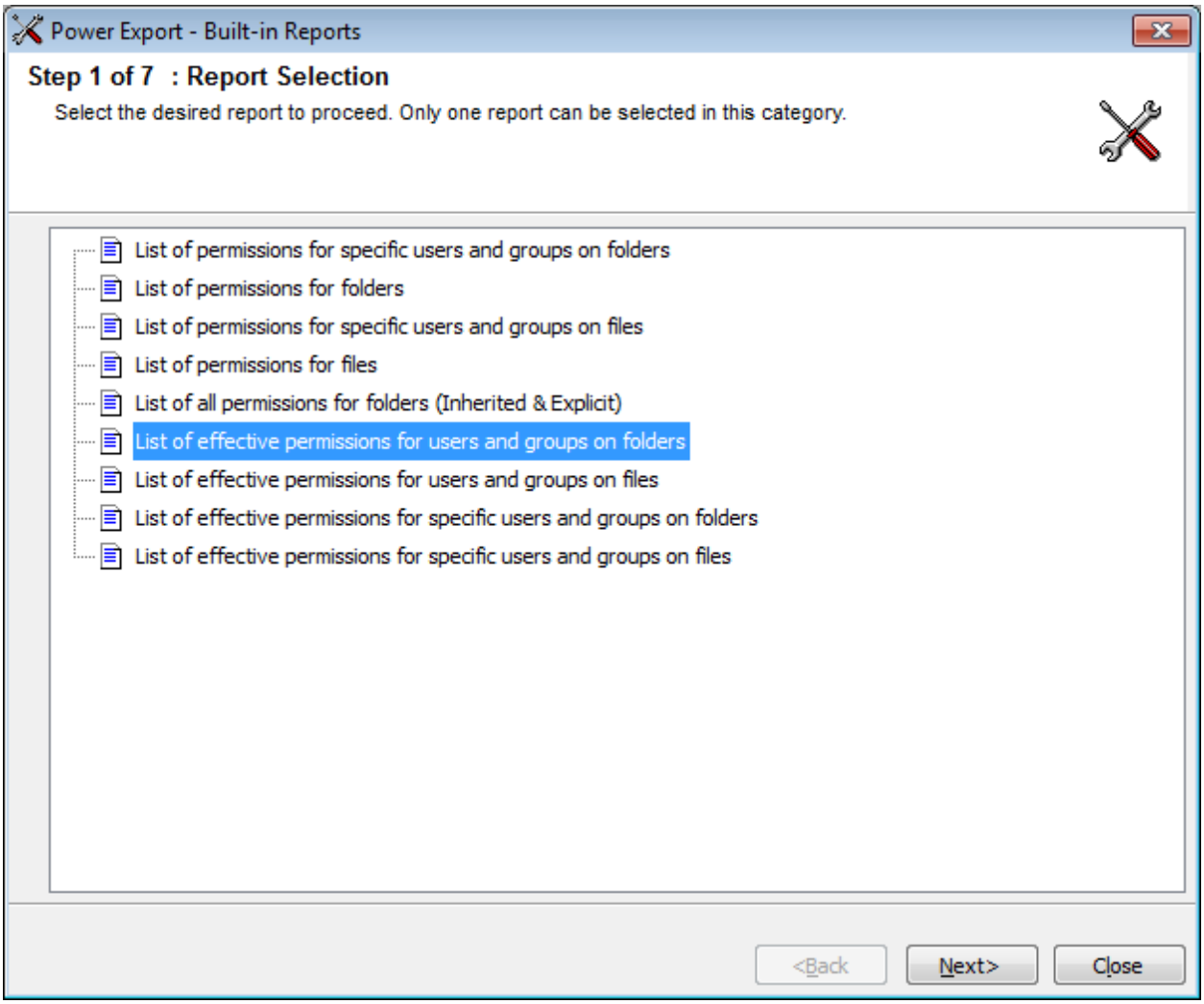
List of effective permission for users and groups on folders

This report lists effective permissions for users and groups assigned to set of folders.

Select

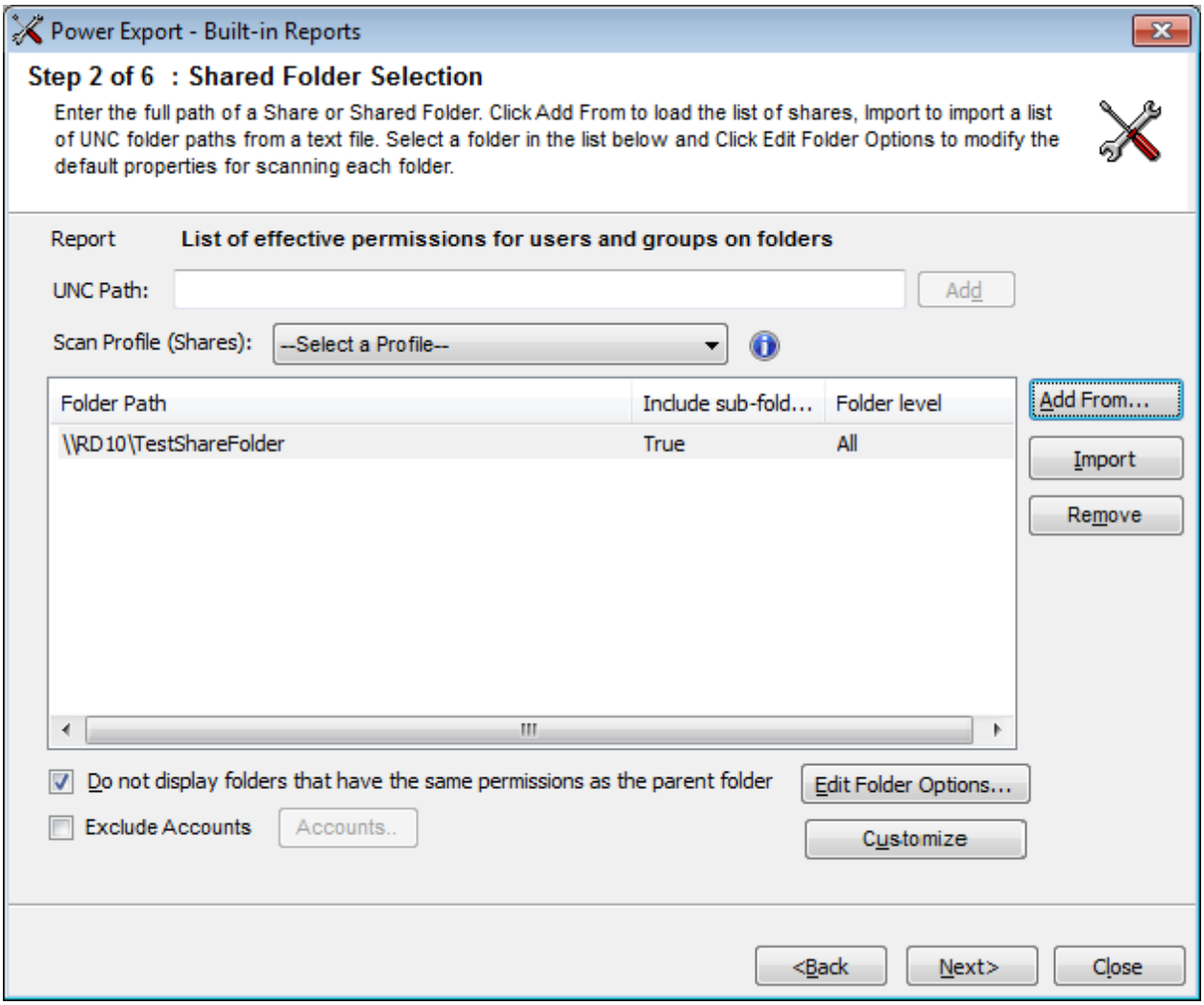
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection


Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

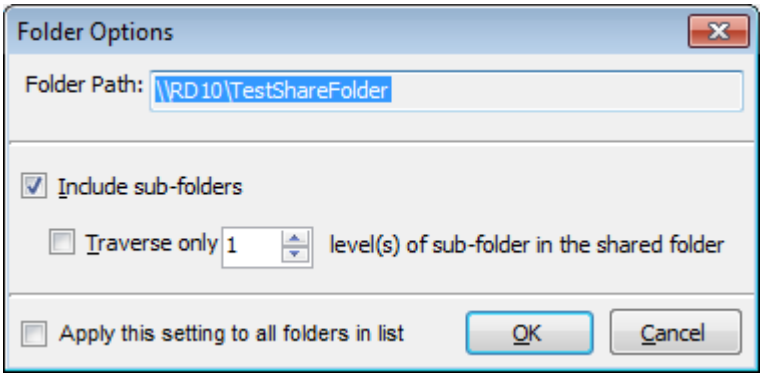
1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: Shared Folder Selection

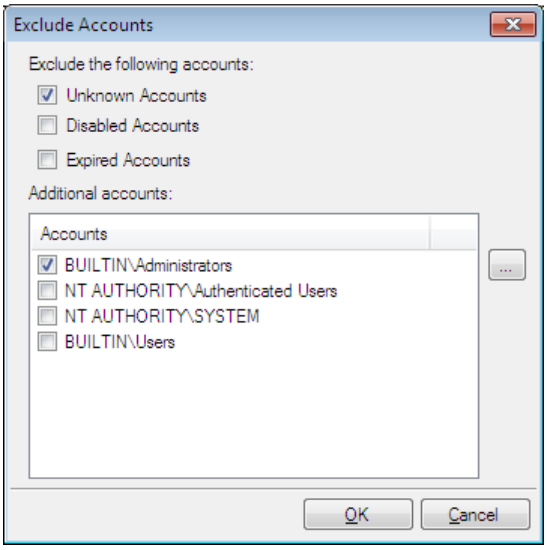

Power Export - Built-in Reports
Step 2 of 6 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of effective permissions for users and groups on folders
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
<Back
Next>
Close

1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.

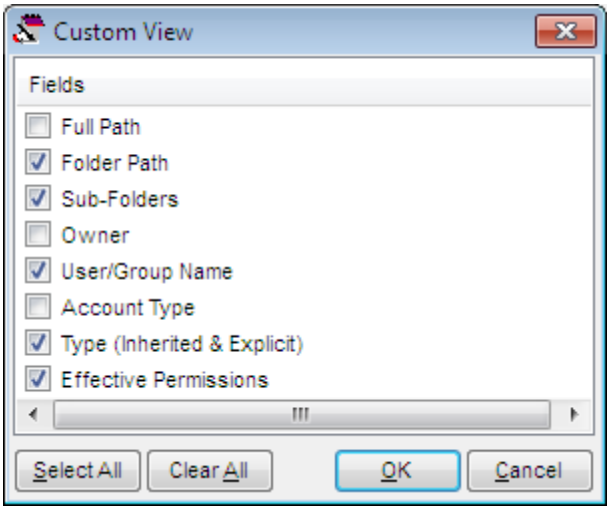
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



5. Modify the folder options as required and click **OK**.
6. If you want to exclude specific accounts select **Exclude Accounts** option. Click **Accounts...** button. That will show up a window as shown below:

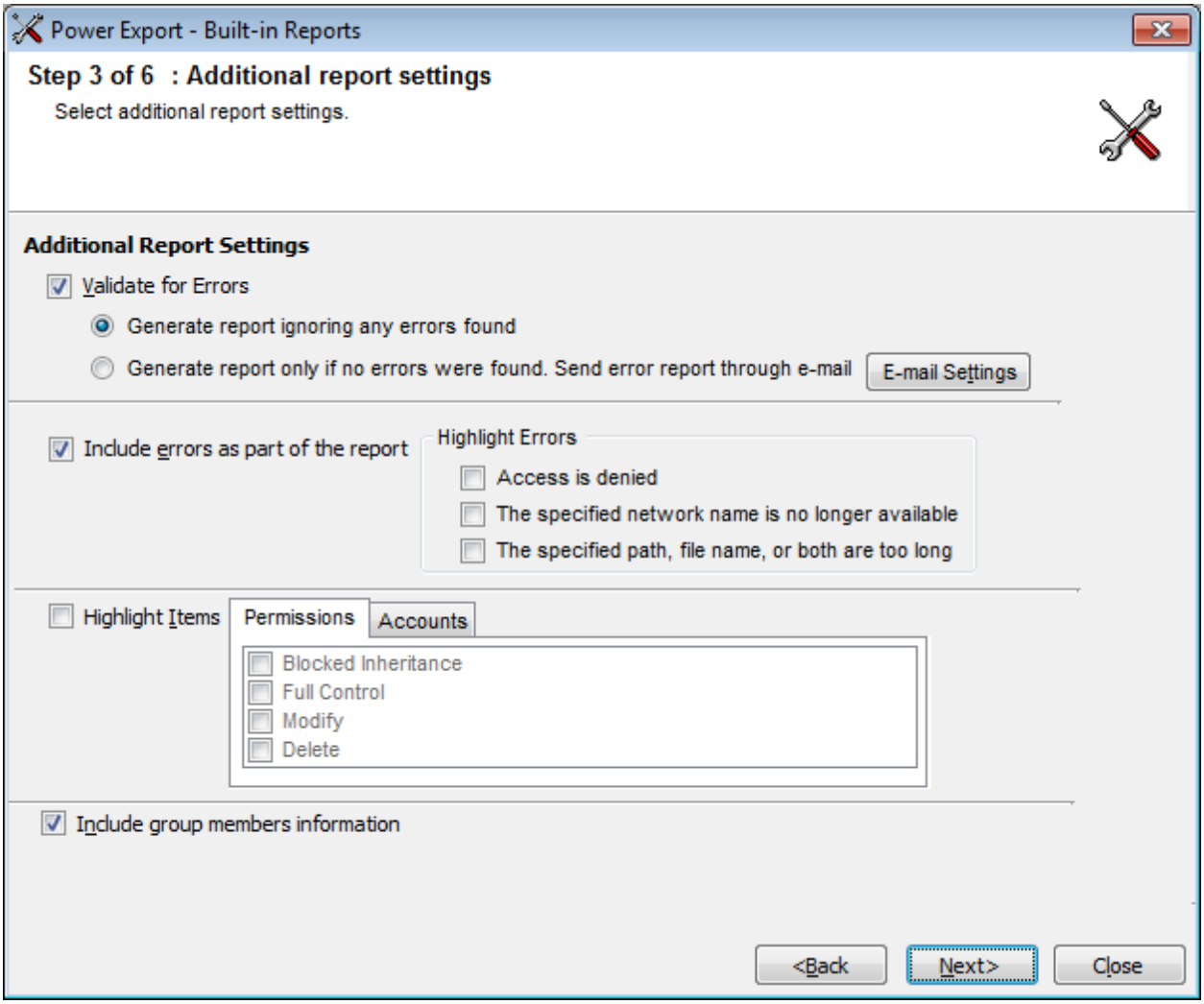


7. Select the accounts for which you want to exclude and click **OK**.
8. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



9. Select the customize options as required and click **OK**.
10. Click **Next** to proceed to the Next step.

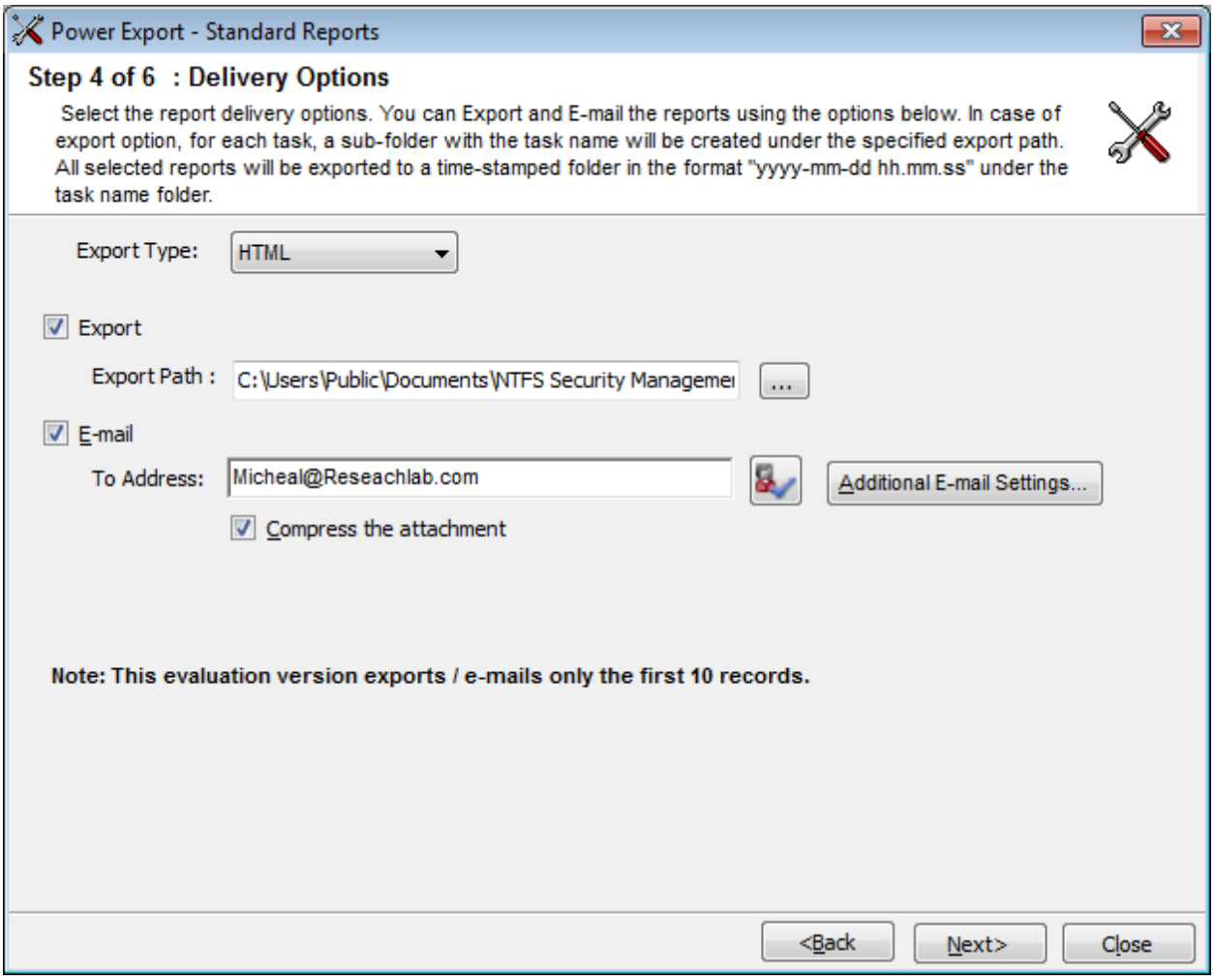
Step 3: Additional report settings


Power Export - Built-in Reports
Step 3 of 6 : Additional report settings
Select additional report settings.
Additional Report Settings
Validate for Errors
Generate report ignoring any errors found
Generate report only if no errors were found. Send error report through e-mail
E-mail Settings
Include errors as part of the report
Highlight Errors
Access is denied
The specified network name is no longer available
The specified path, file name, or both are too long
Highlight Items
Permissions
Accounts
Blocked Inheritance
Full Control
Modify
Delete
Include group members information
<Back
Next>
Close

1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

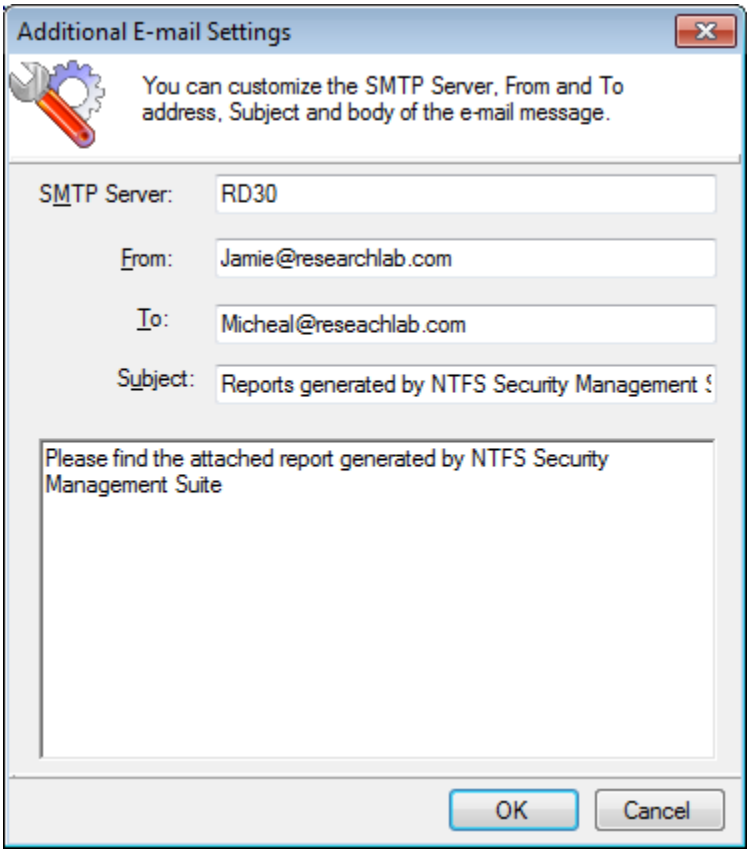
4. You may also select **Include group members information** for include members of group and their sub-group members at all group levels in the report.
5. Click **Next** to proceed to the Next step.

Step 4: Delivery Options

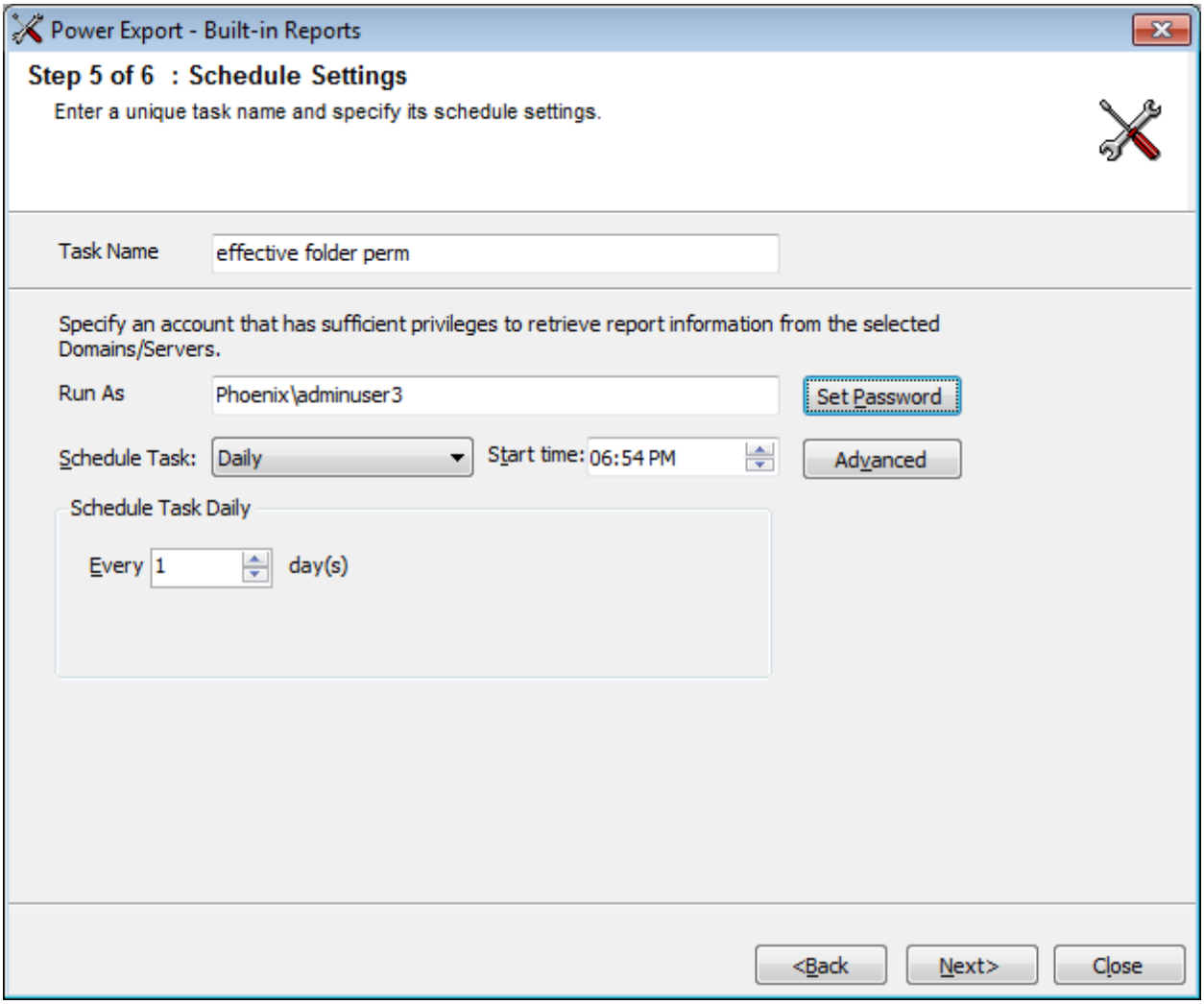

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

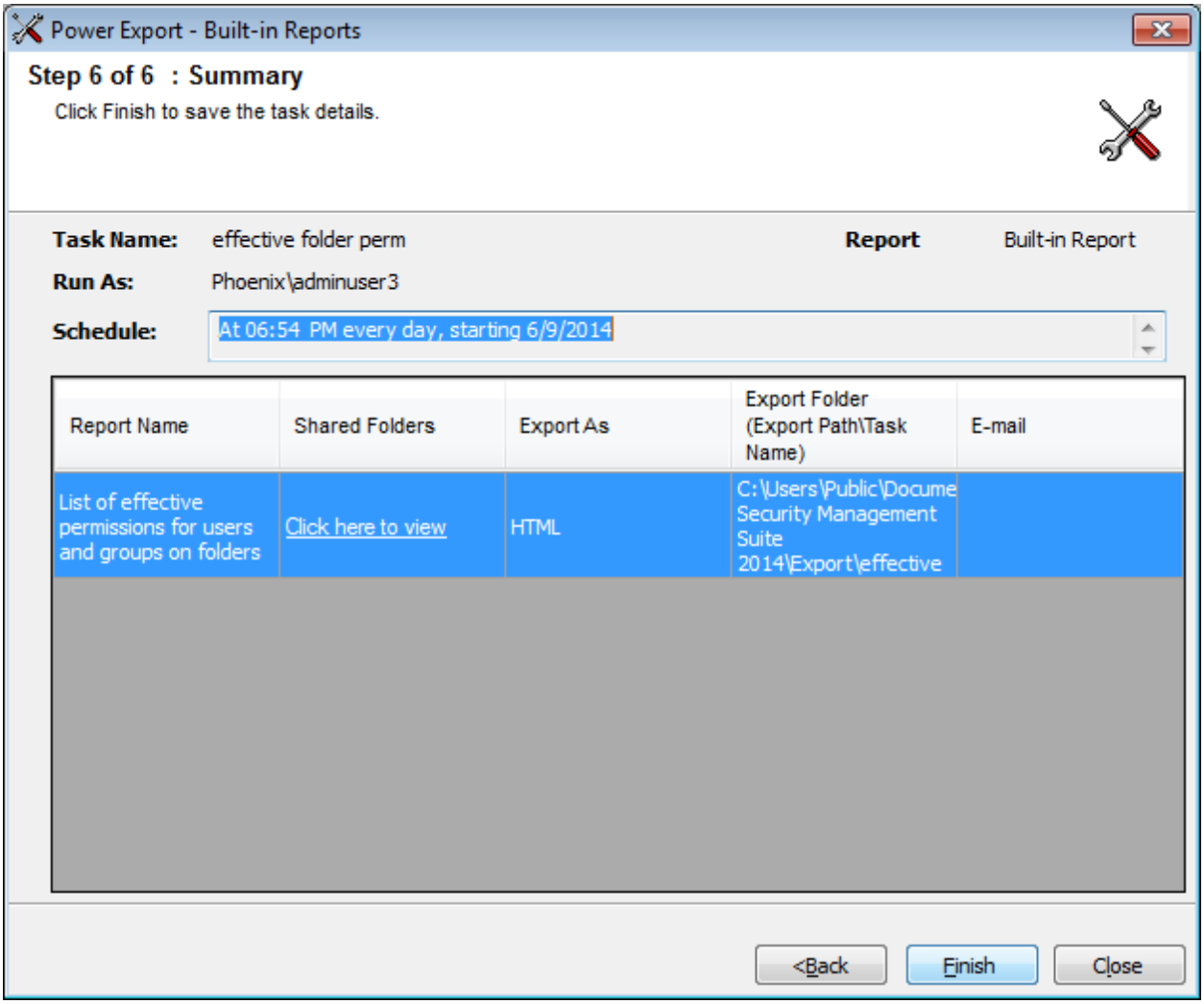

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

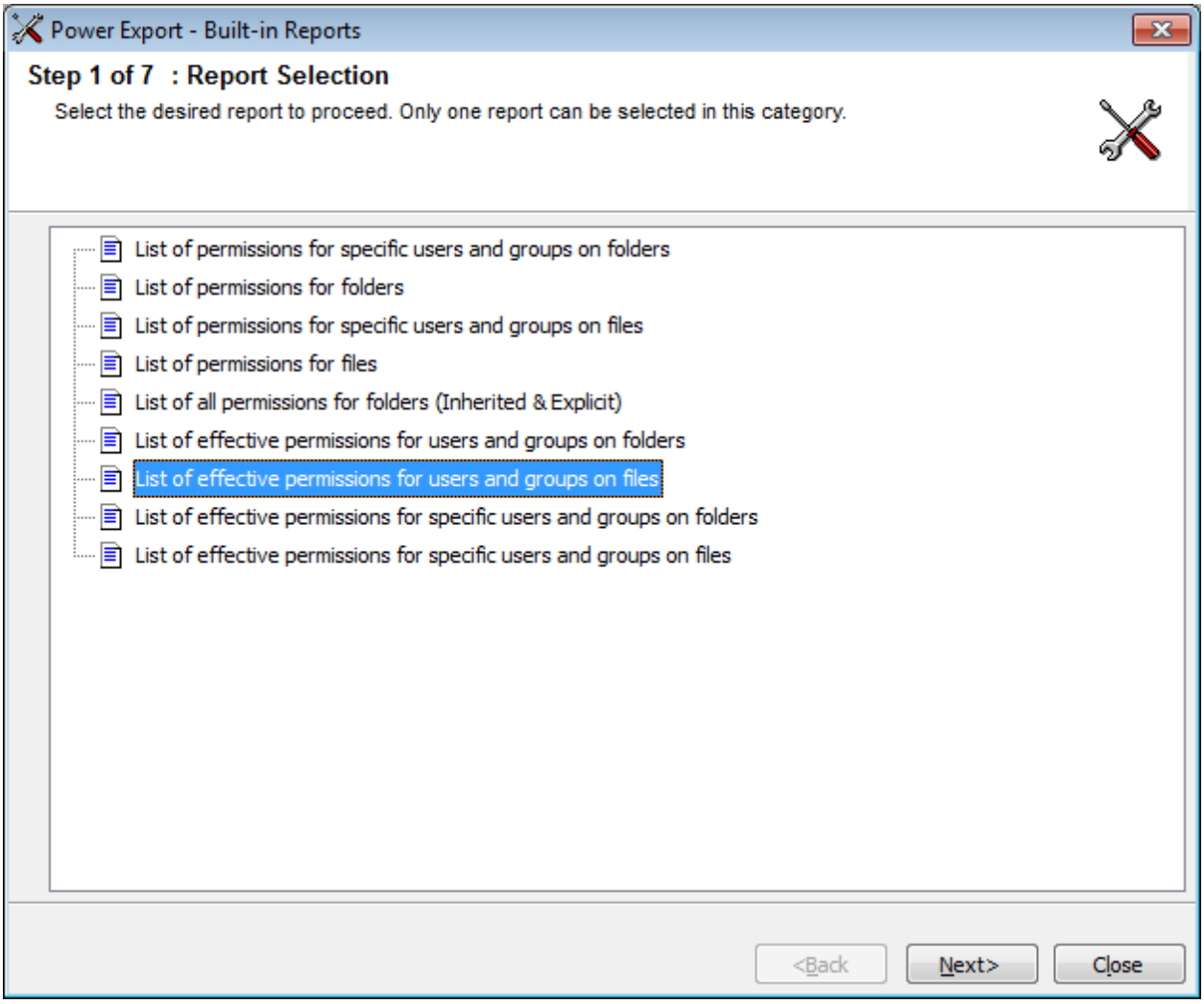
List of effective permission for users and groups on files

This report lists effective permissions for users and groups assigned to files available in a set of folders.

Select

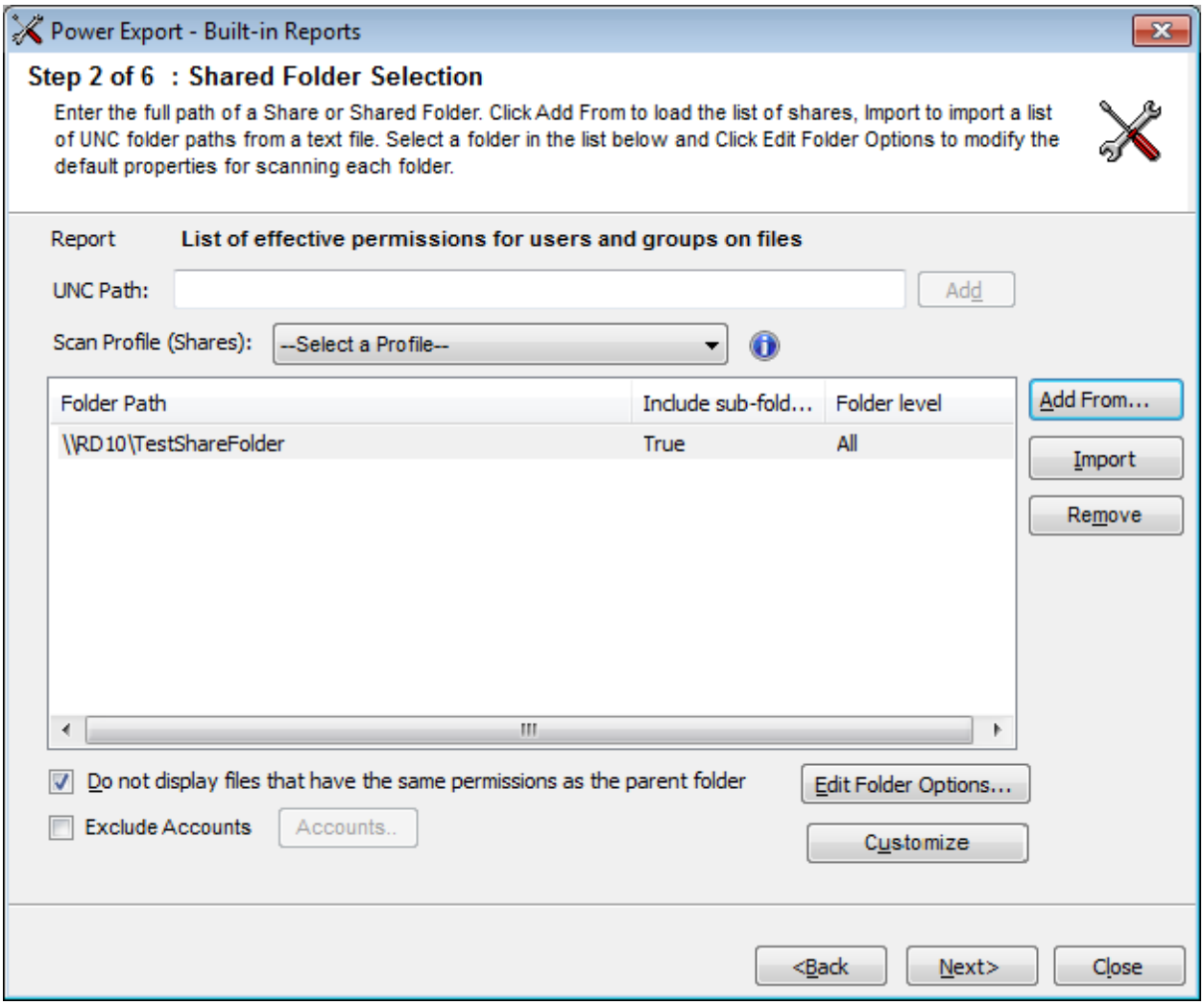
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection

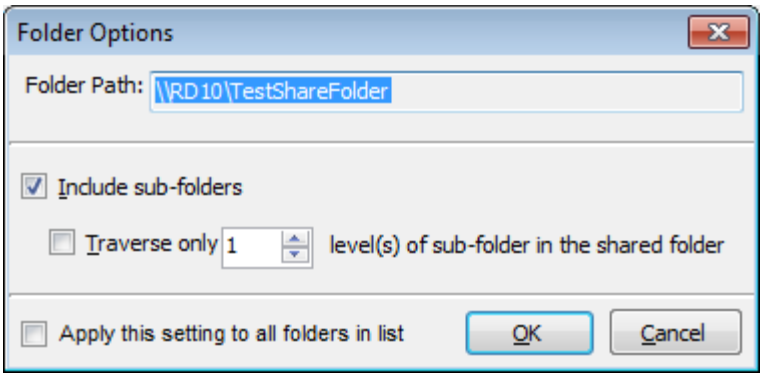

Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

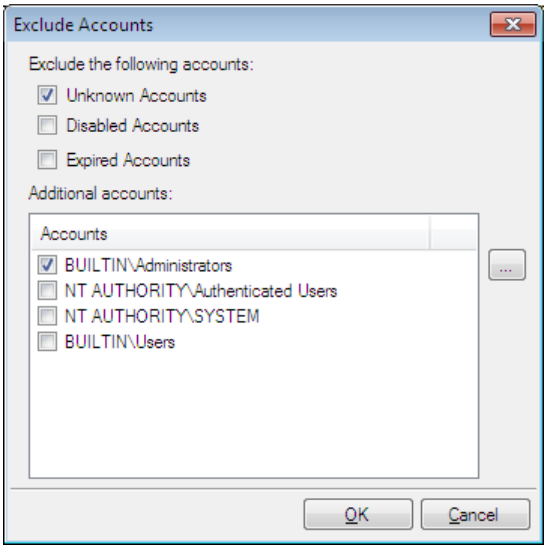
Step 2: Shared Folder Selection


Power Export - Built-in Reports
Step 2 of 6 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of effective permissions for users and groups on files
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display files that have the same permissions as the parent folder
Edit Folder Options...
Exclude Accounts
Accounts..
Customize
<Back
Next>
Close

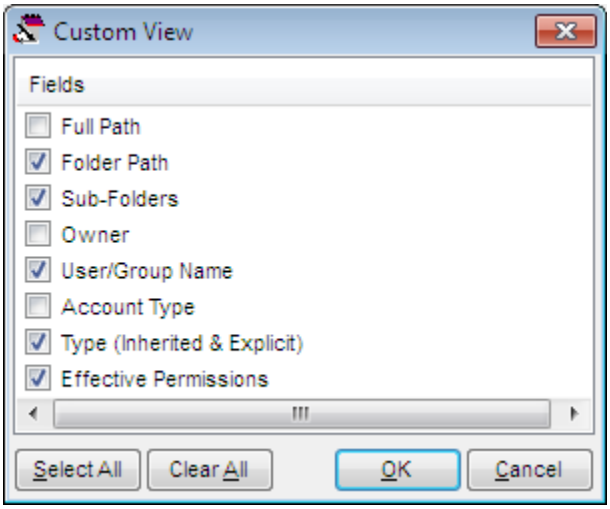
1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



5. Modify the folder options as required and click **OK**.
6. If you want to exclude specific accounts select **Exclude Accounts** option. Click **Accounts...** button. That will show up a window as shown below:



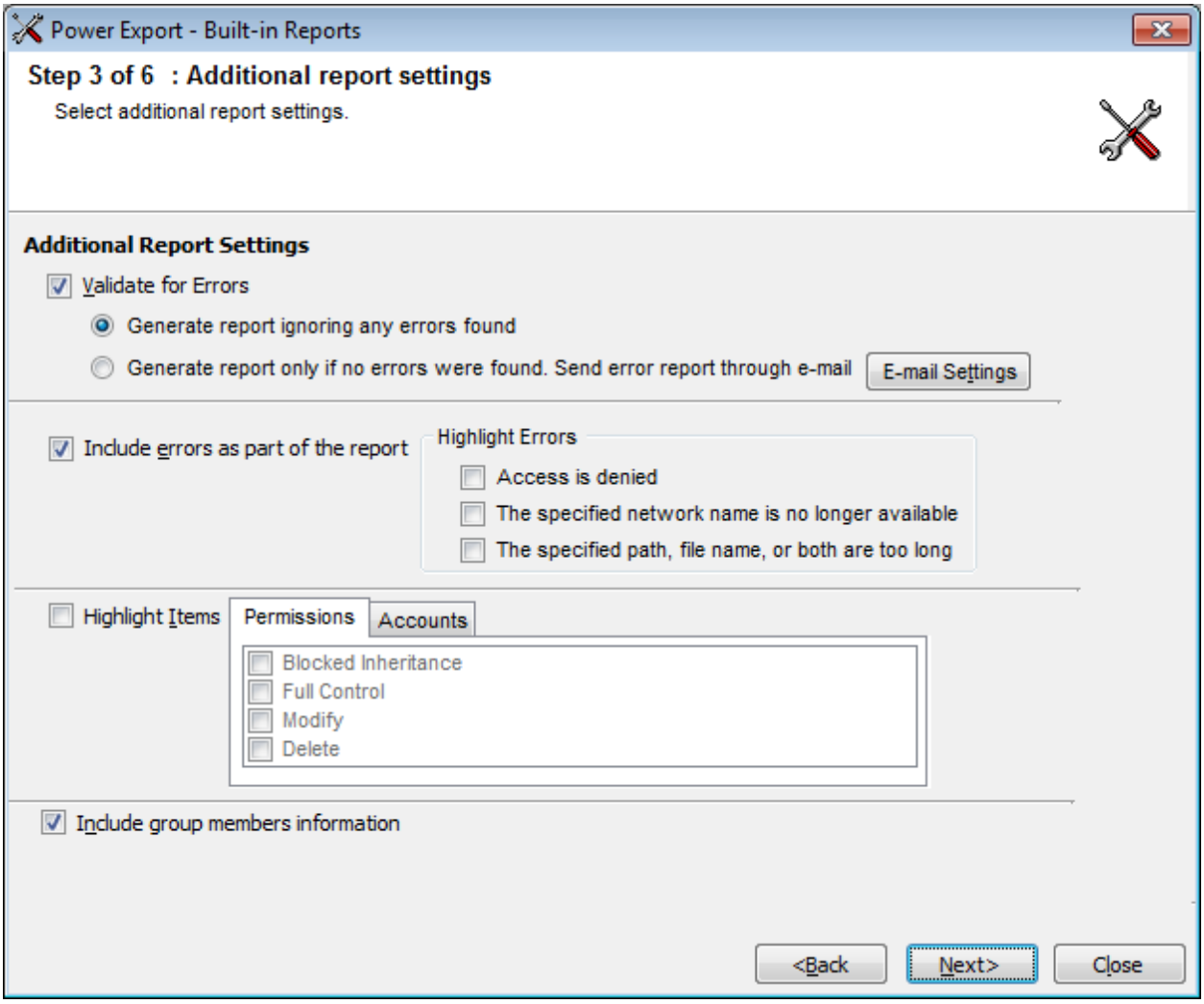
7. Select the accounts for which you want to exclude and click **OK**.
8. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



9. Select the customize options as required and click **OK**.

10. Click **Next** to proceed to the Next step.

Step 3: Additional report settings


Power Export - Built-in Reports
Step 3 of 6 : Additional report settings
Select additional report settings.
Additional Report Settings
Validate for Errors
Generate report ignoring any errors found
Generate report only if no errors were found. Send error report through e-mail
E-mail Settings
Include errors as part of the report
Highlight Errors
Access is denied
The specified network name is no longer available
The specified path, file name, or both are too long
Highlight Items
Permissions
Accounts
Blocked Inheritance
Full Control
Modify
Delete
Include group members information
<Back
Next>
Close

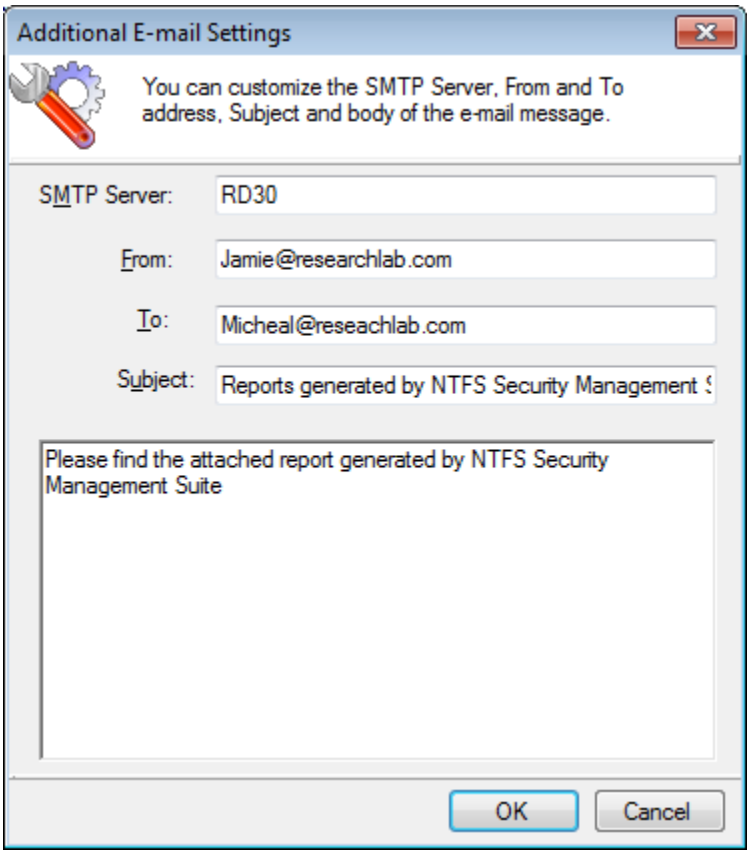
1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select the error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

4. You may also select **Include group members information** for include members of a group and their sub-group members at all group levels in the report.
5. Click **Next** to proceed to the Next step.

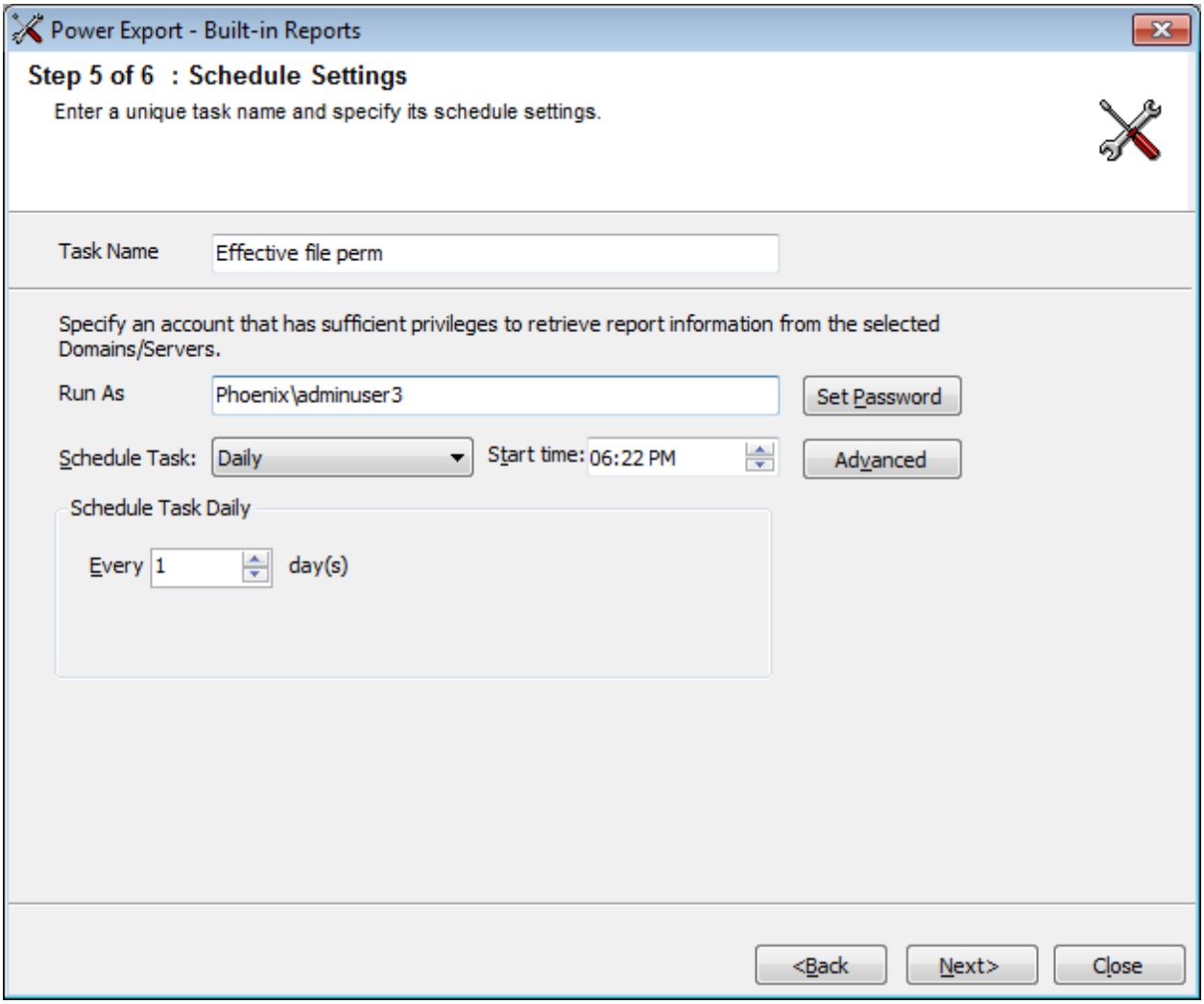
Step 4: Delivery Options

1. Change the Export or Print or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

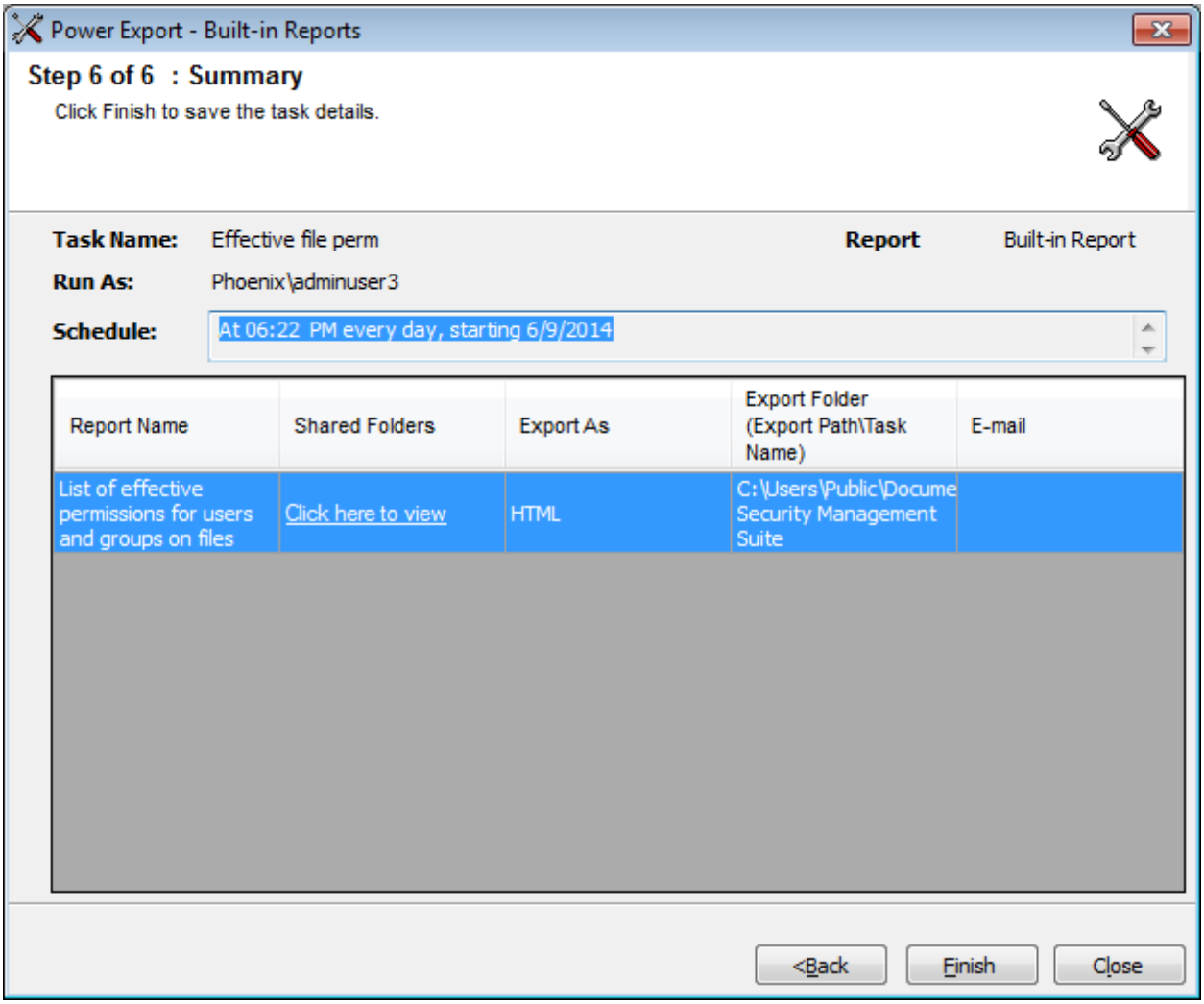


Step 5: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

List of effective permissions for specific users and groups on folders

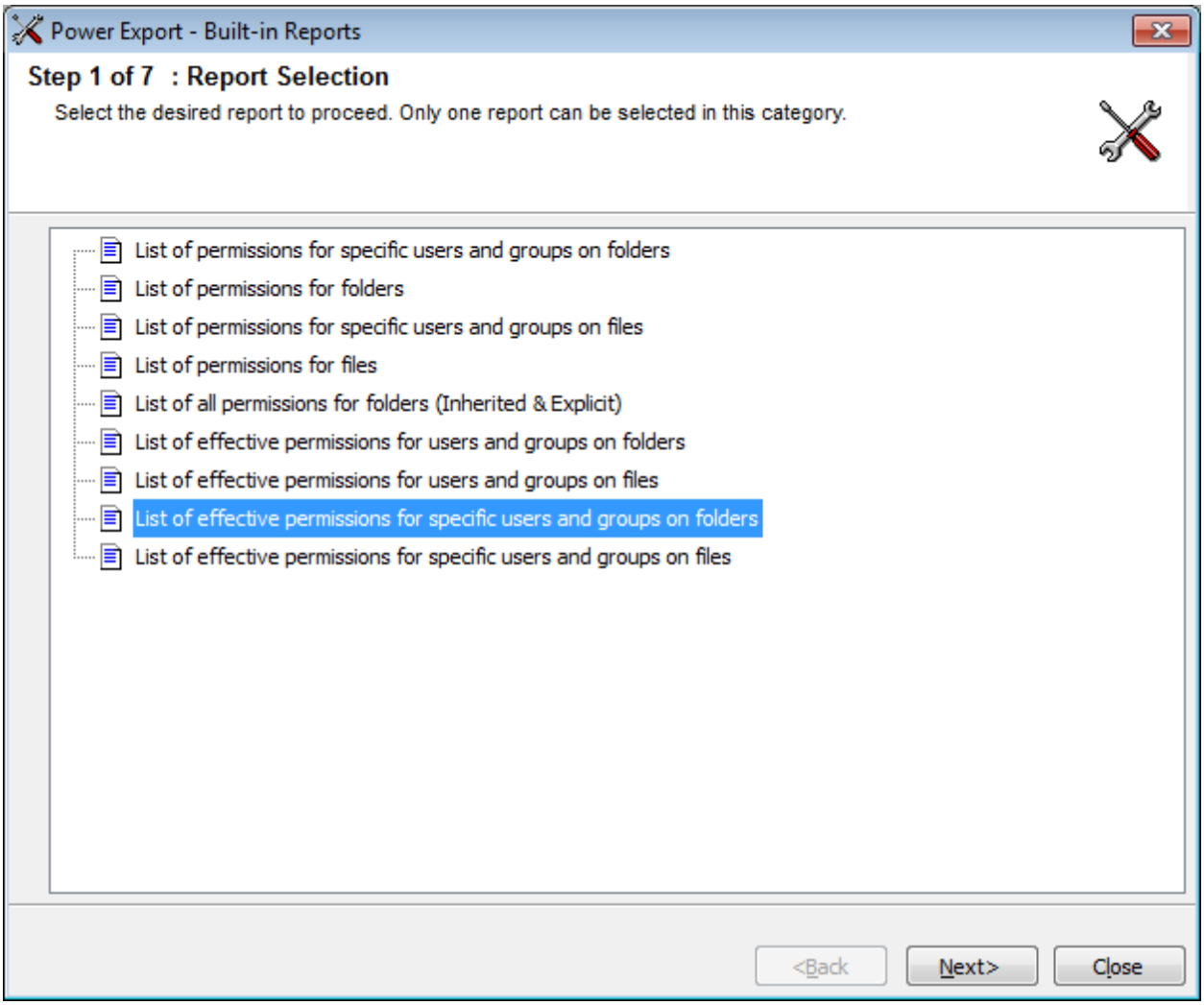
---

This report lists effective permissions for specific users and groups assigned to set of folders.

Select

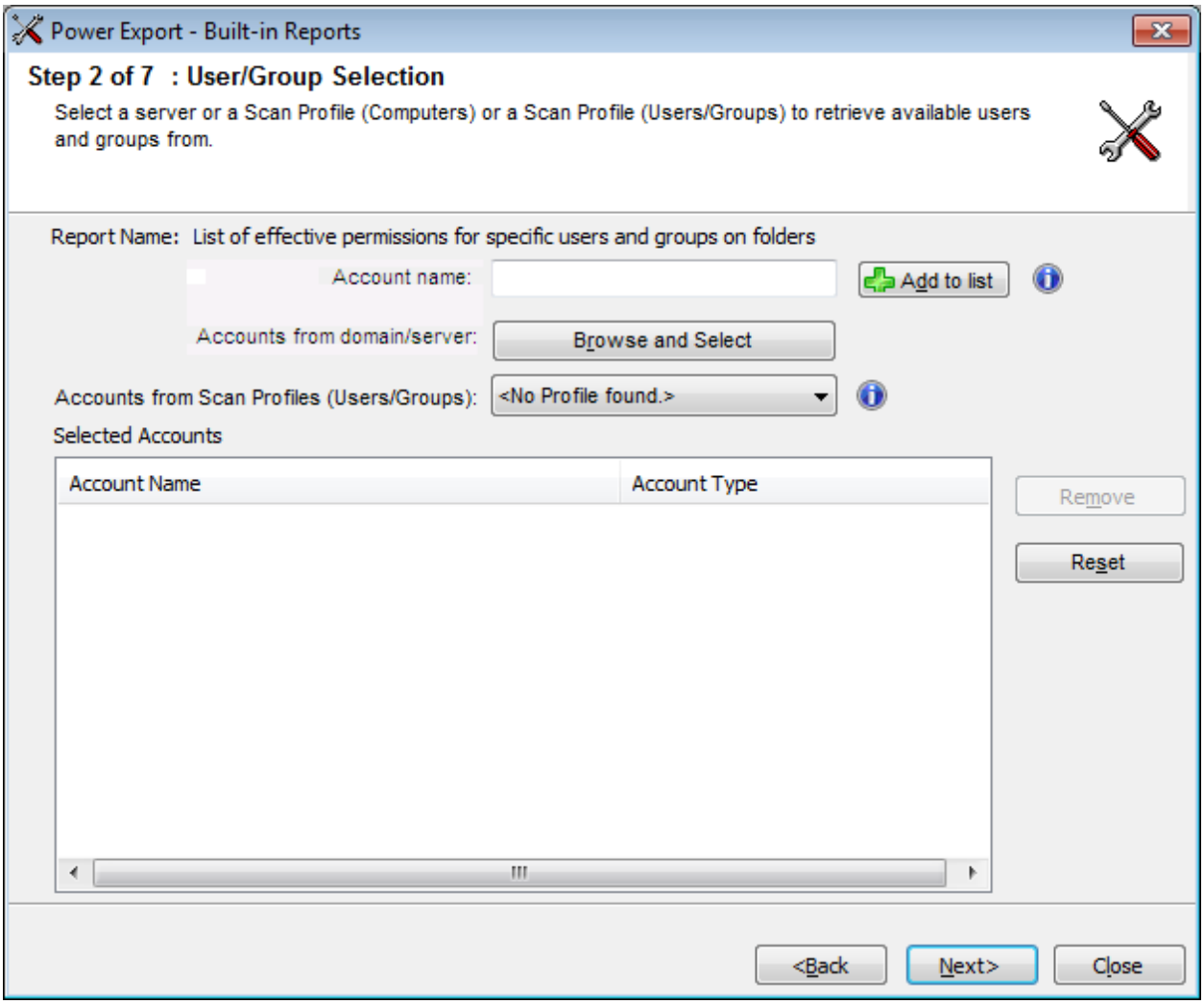
option under Power Export. This will bring up the Power Export Wizard.

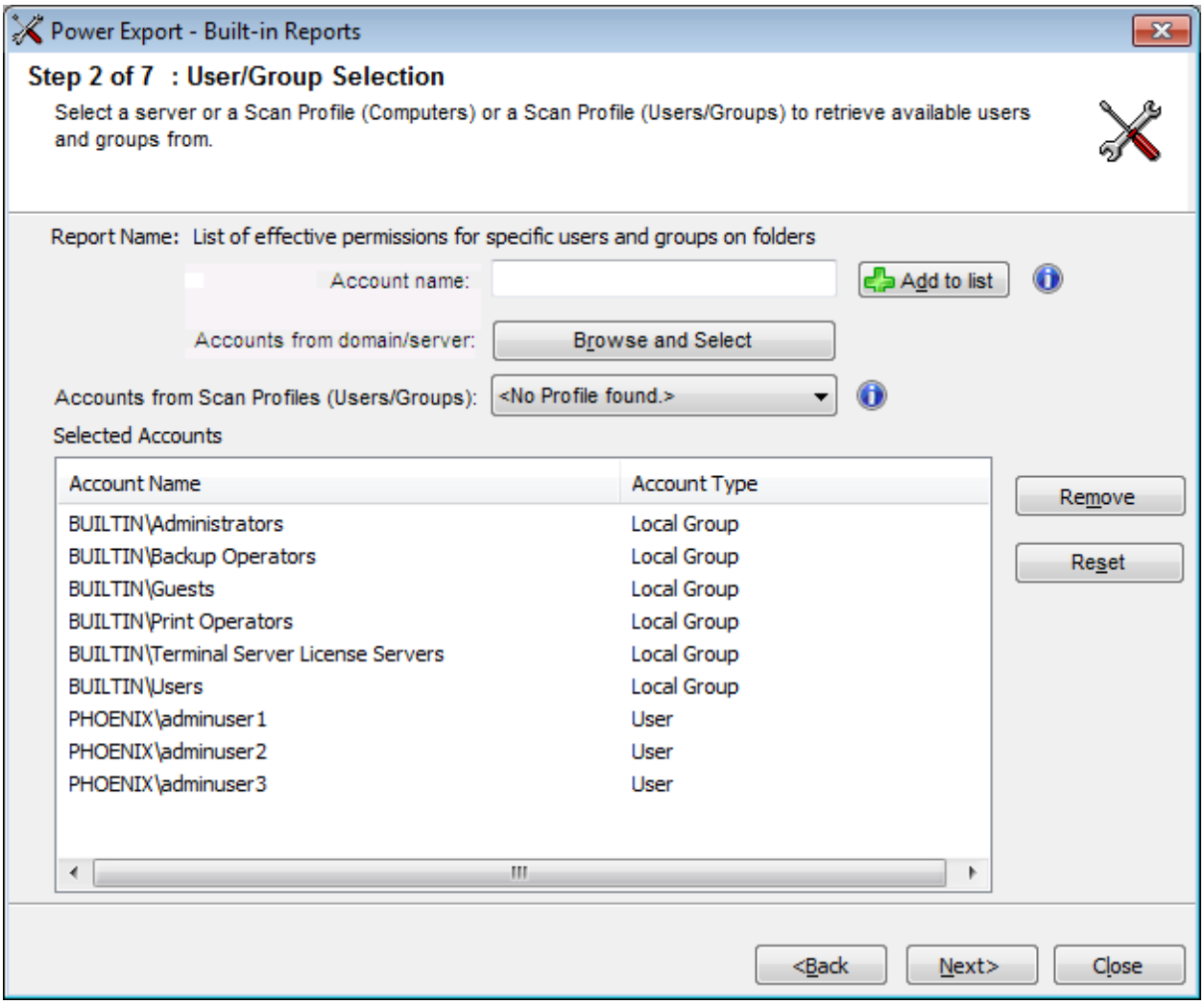
Step 1: Report Selection


Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: User and/or Group Selection

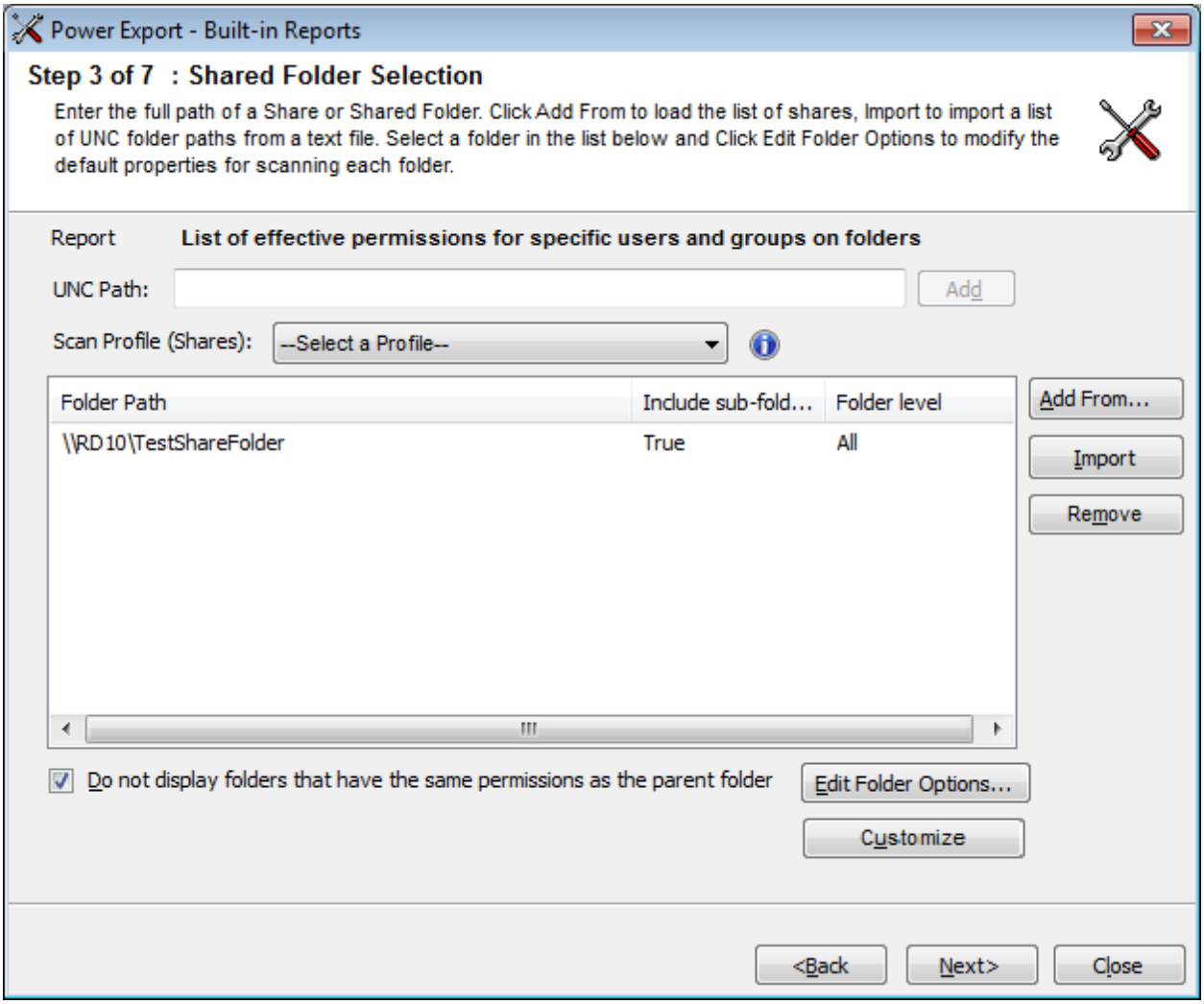

Power Export - Built-in Reports
Step 2 of 7 : User/Group Selection
Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.
Report Name: List of effective permissions for specific users and groups on folders
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
<No Profile found.>
Selected Accounts
Account Name
Account Type
Remove
Reset
<Back
Next>
Close



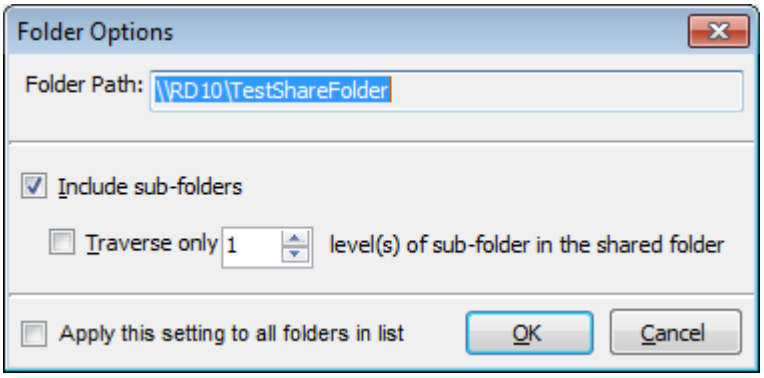
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

1. Select the user or group, for which you wish to run the permissions report.
2. The selected users will be added to the wizard as shown above:
3. Click **Next** to proceed to the Next step.

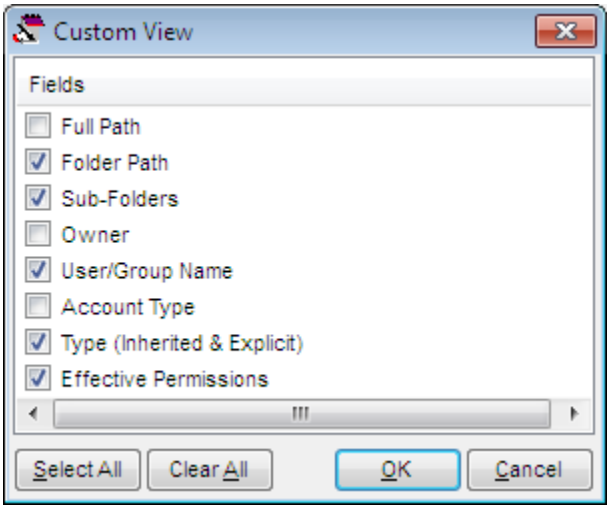
Step 3: Shared Folder Selection


Power Export - Built-in Reports
Step 3 of 7 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of effective permissions for specific users and groups on folders
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Customize
<Back
Next>
Close

1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder option**. This option will not report folders with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:

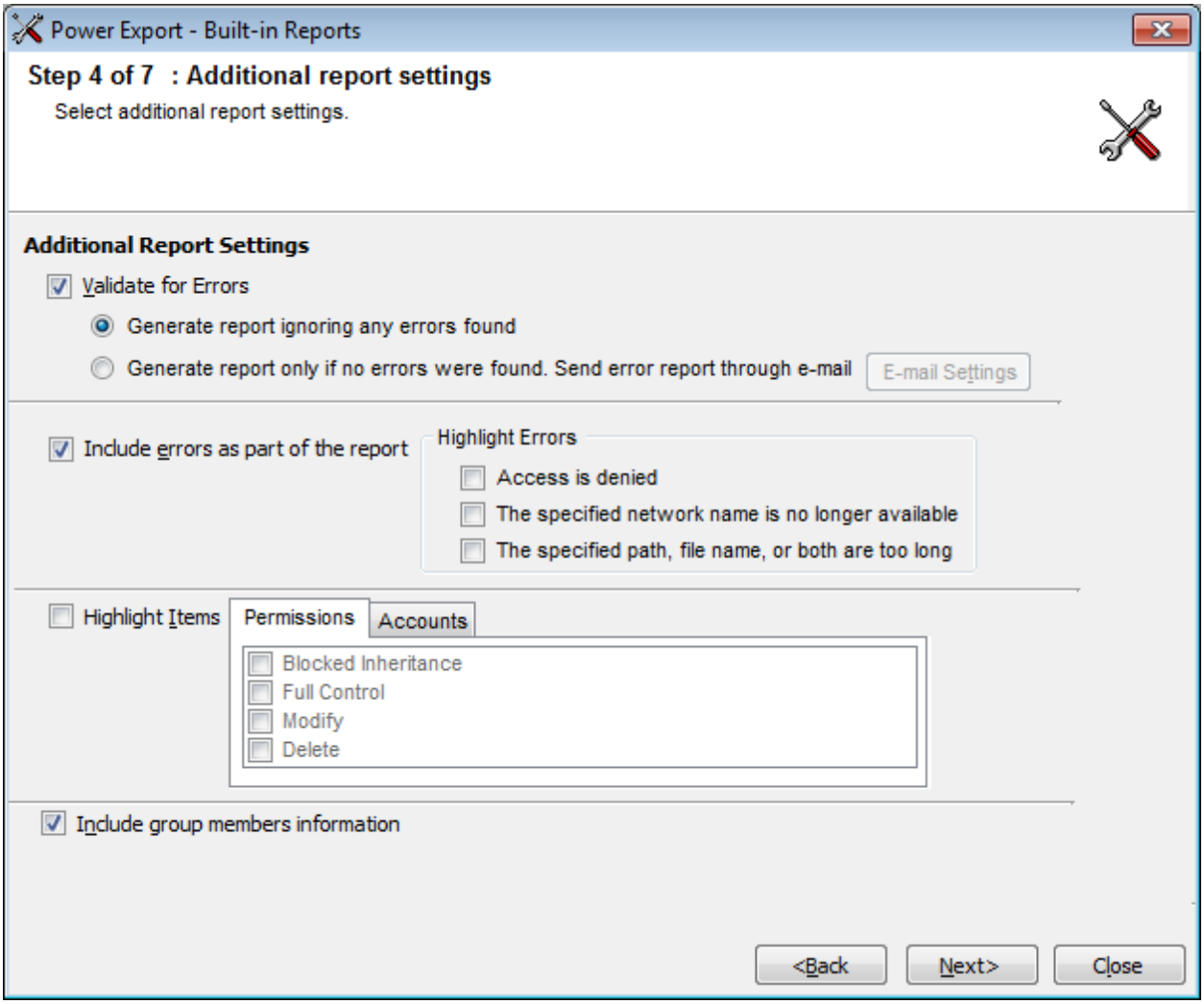


5. Modify the folder options as required and click **OK**.
6. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



7. Select the customize options as required and click **OK**.
8. Click **Next** to proceed to the Next step.

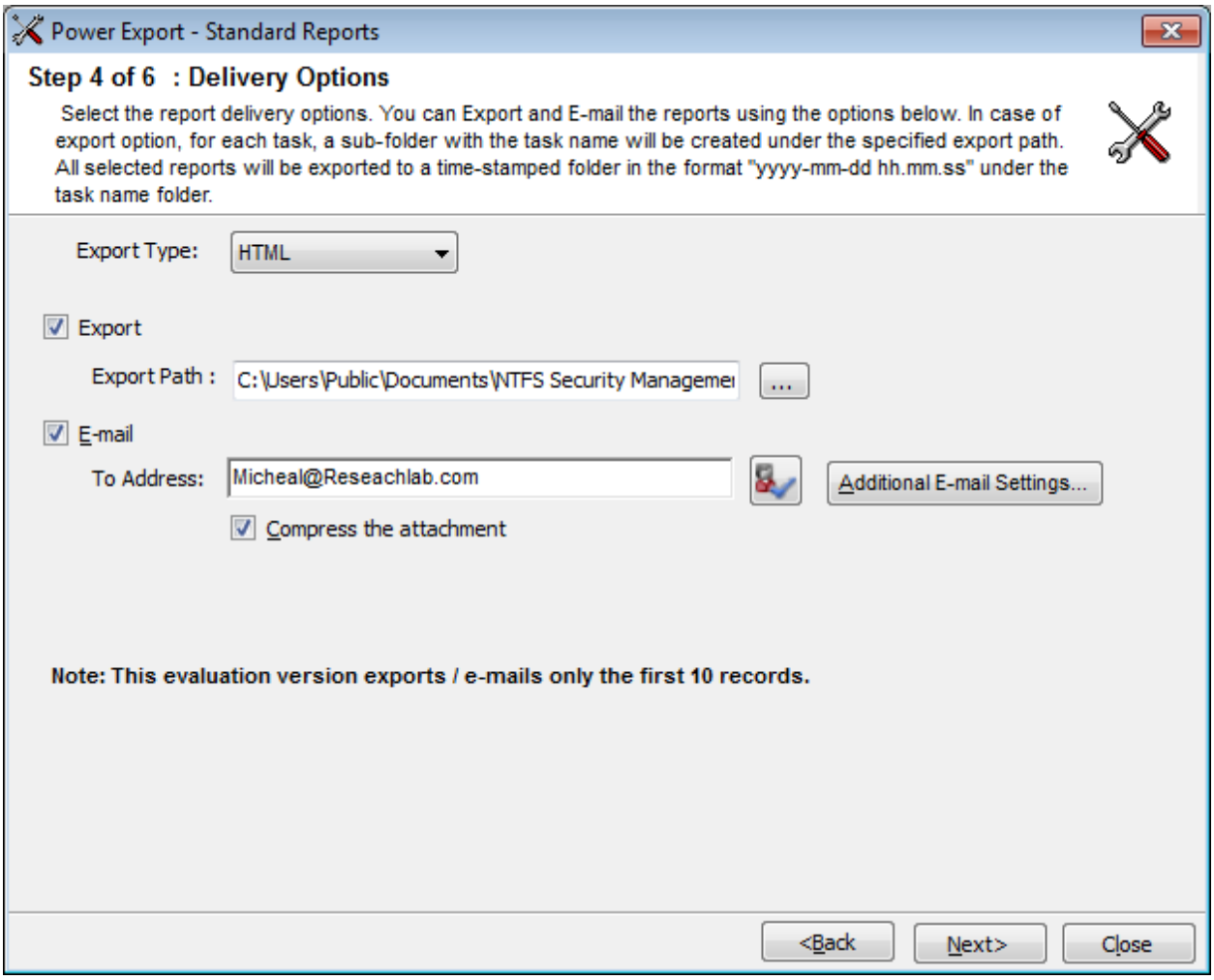
Step 4: Additional report settings


Power Export - Built-in Reports
Step 4 of 7 : Additional report settings
Select additional report settings.
Additional Report Settings
Validate for Errors
Generate report ignoring any errors found
Generate report only if no errors were found. Send error report through e-mail
E-mail Settings
Include errors as part of the report
Highlight Errors
Access is denied
The specified network name is no longer available
The specified path, file name, or both are too long
Highlight Items
Permissions
Accounts
Blocked Inheritance
Full Control
Modify
Delete
Include group members information
<Back
Next>
Close

1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

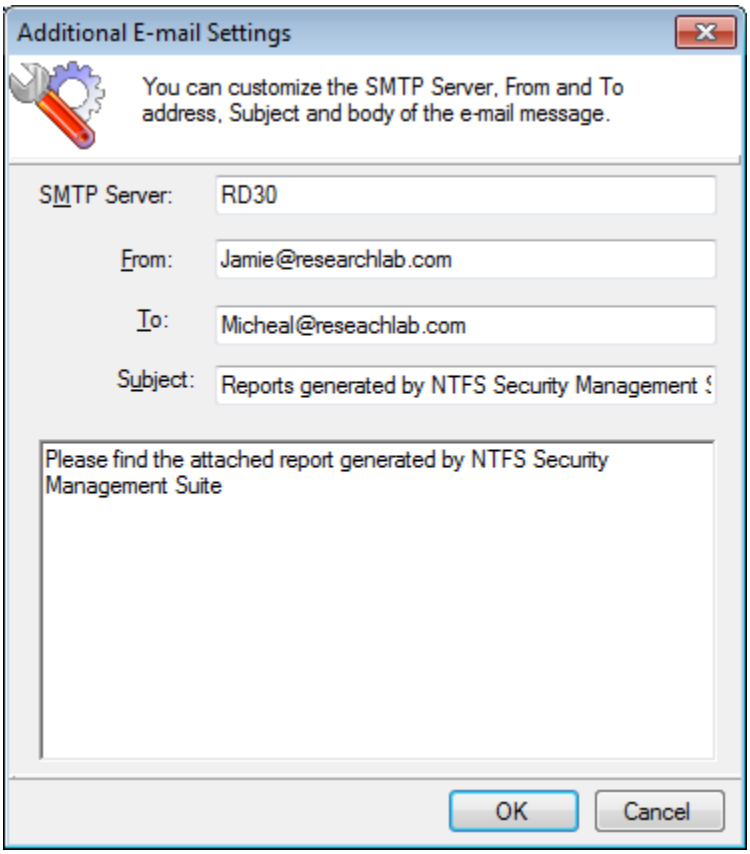
4. You may also select **Include group members information** for include members of a group and their sub-group members at all group levels in the report.
5. Click **Next** to proceed to the Next step.

Step 5: Delivery Options

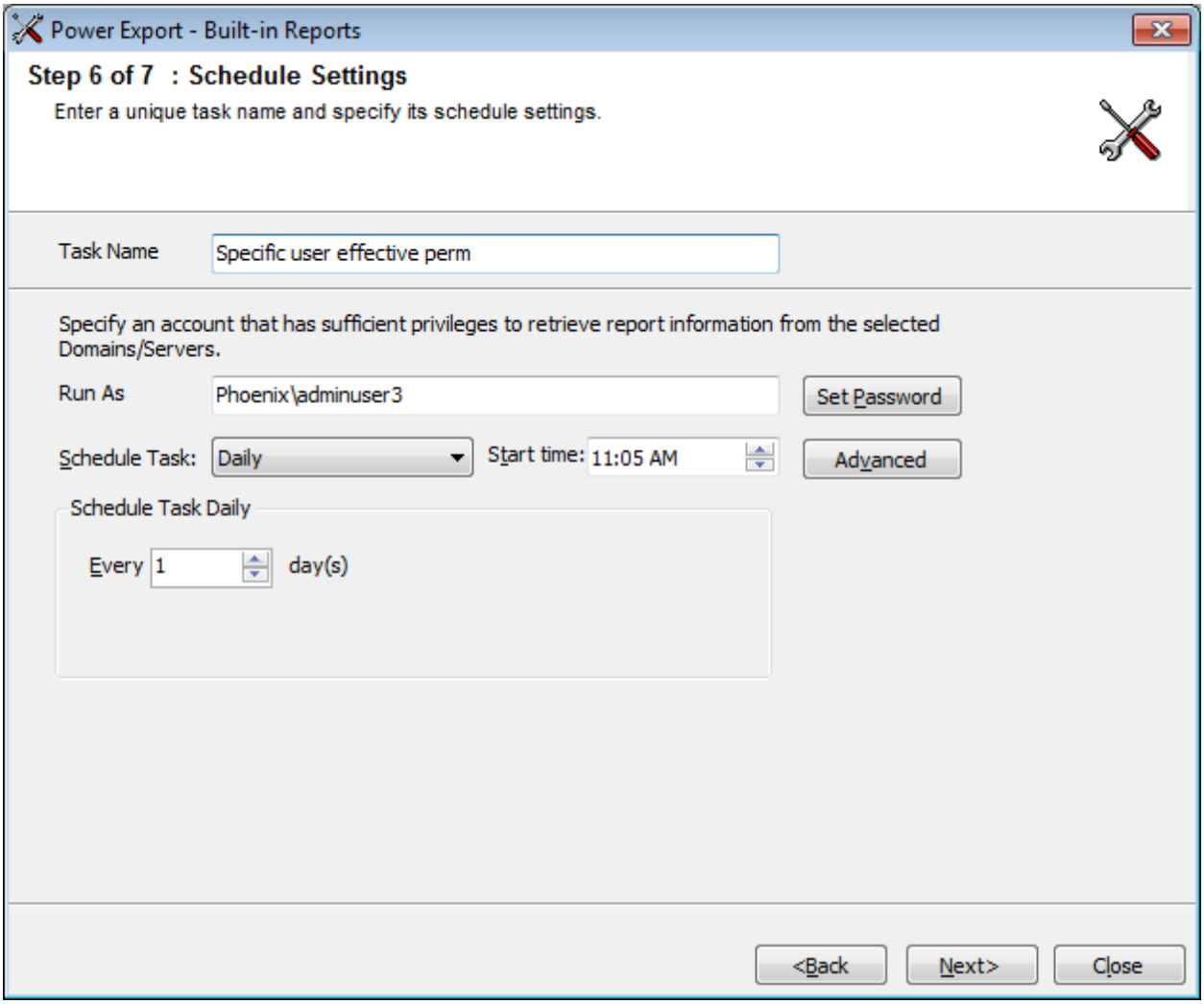

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

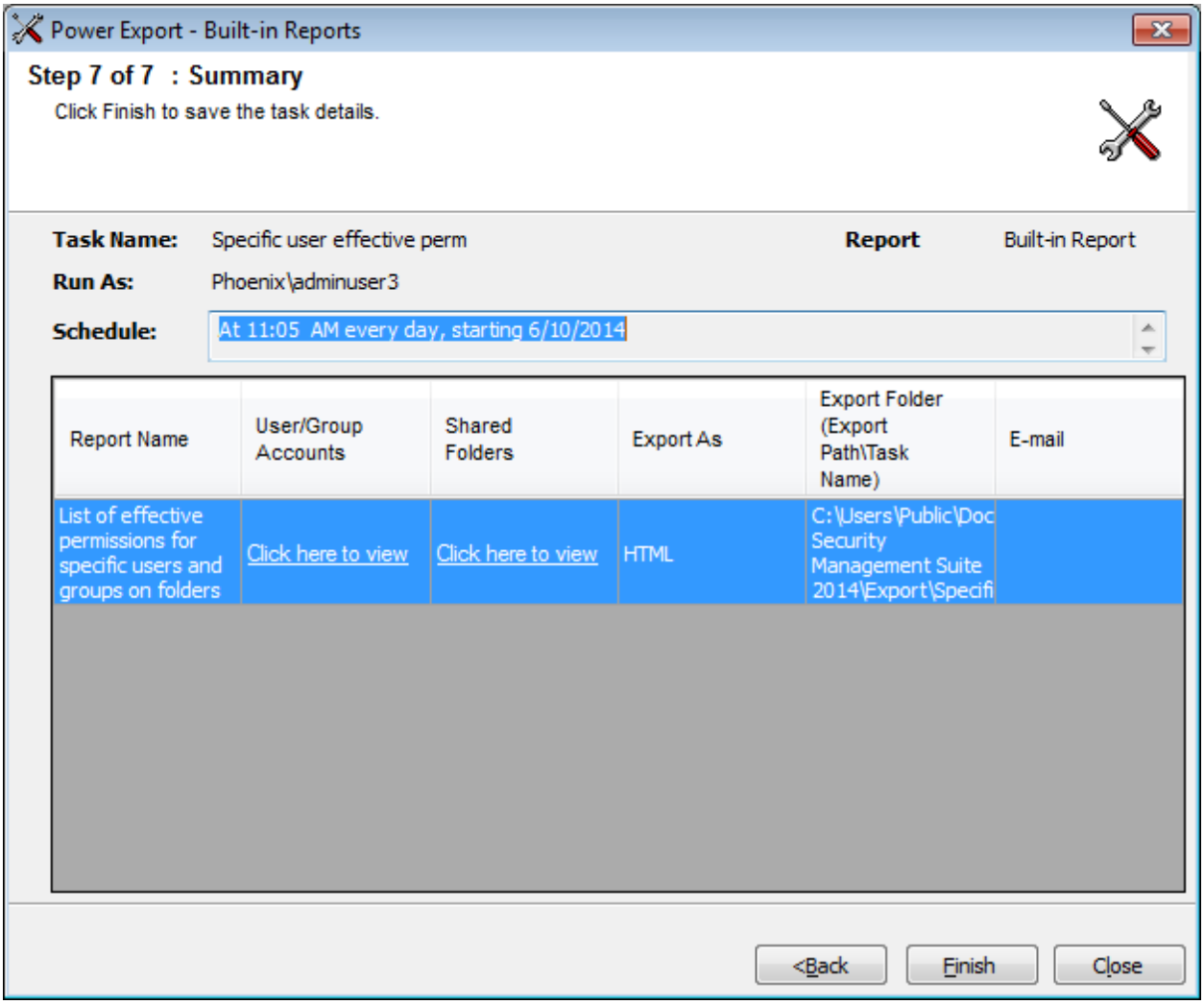


Step 6: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 7: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks.

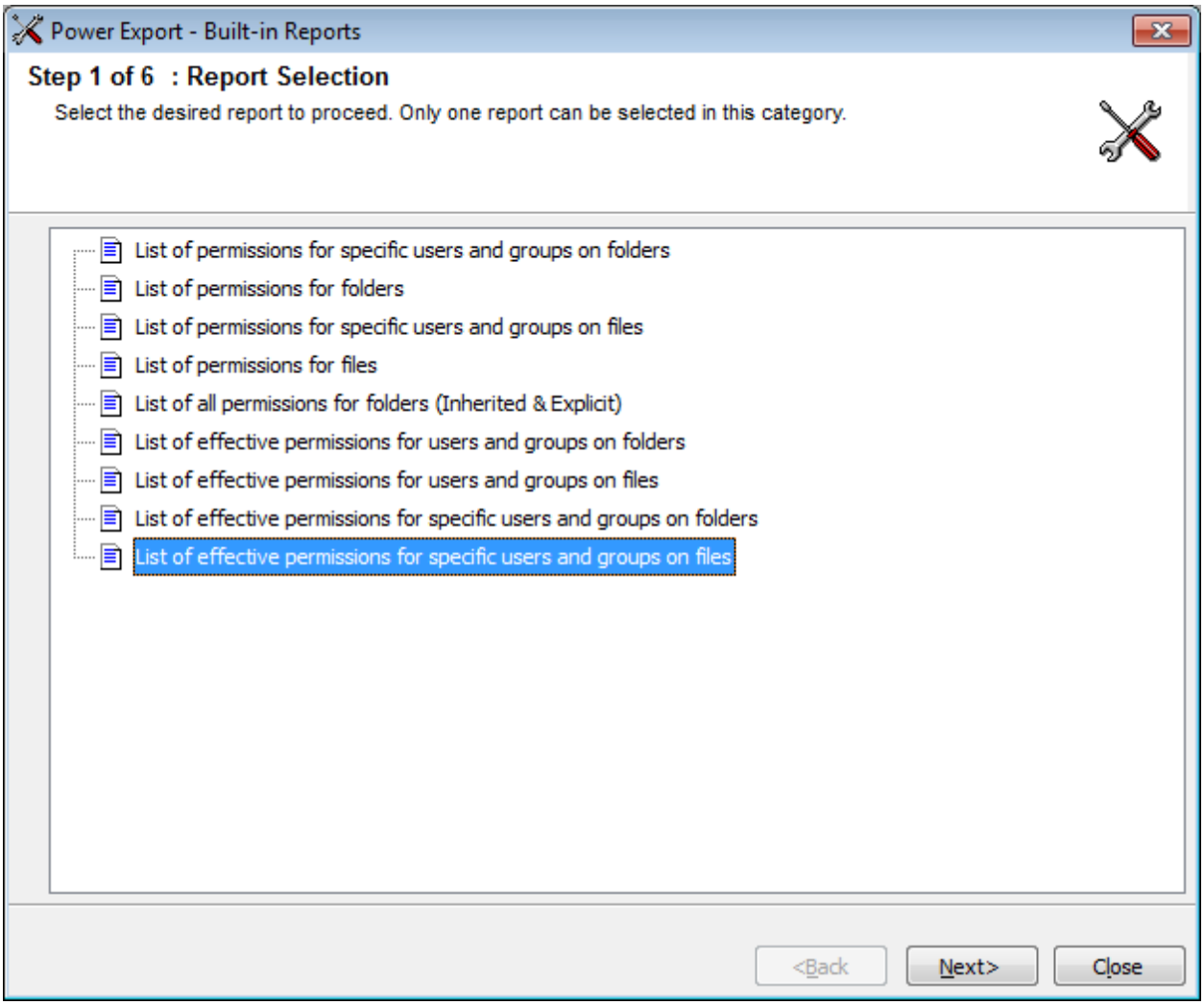
List of effective permissions for specific users and groups on files

This report lists effective permissions for specific users and groups assigned to files available in a set of folders.

Select

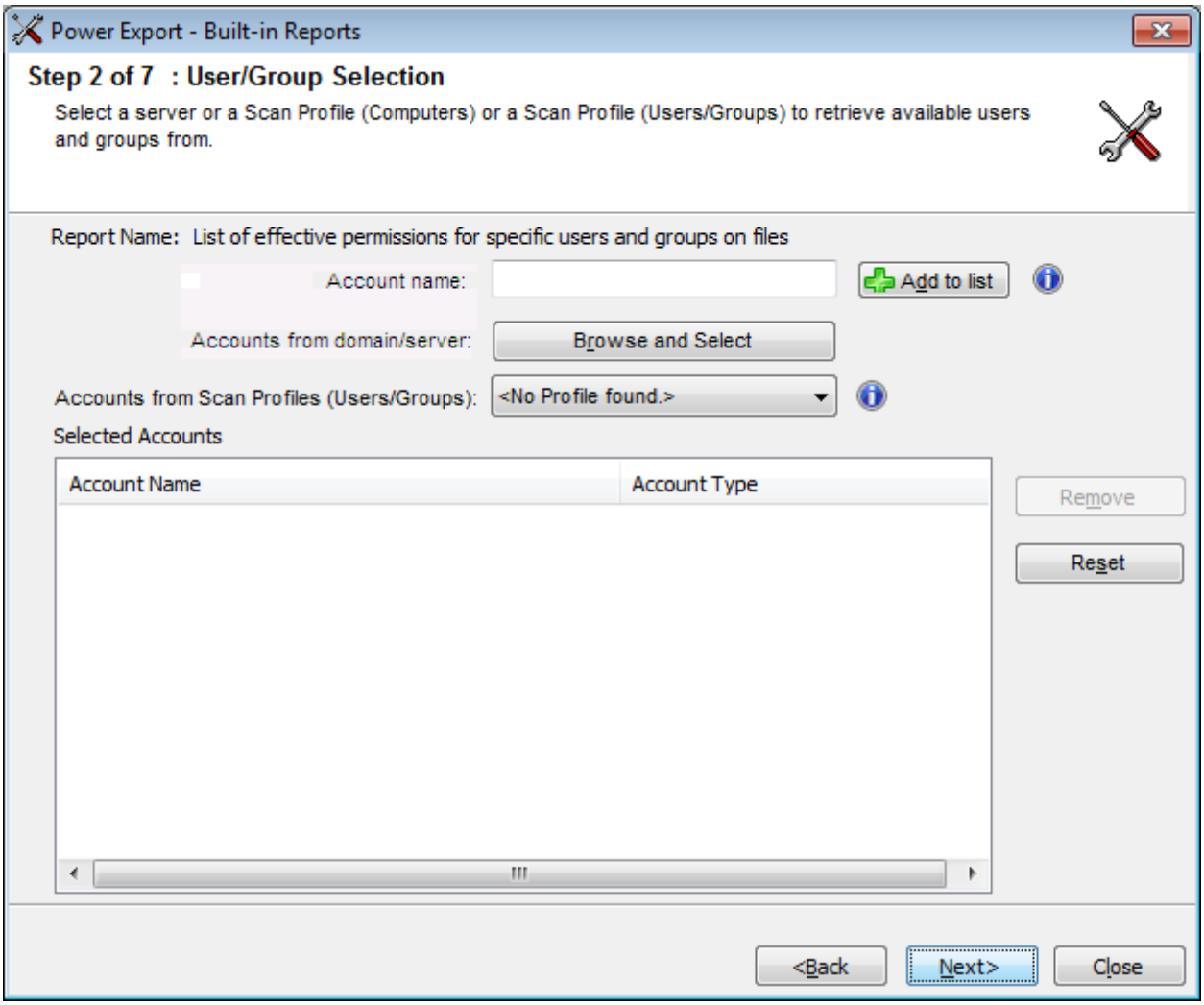
option under Power Export. This will bring up the Power Export Wizard.

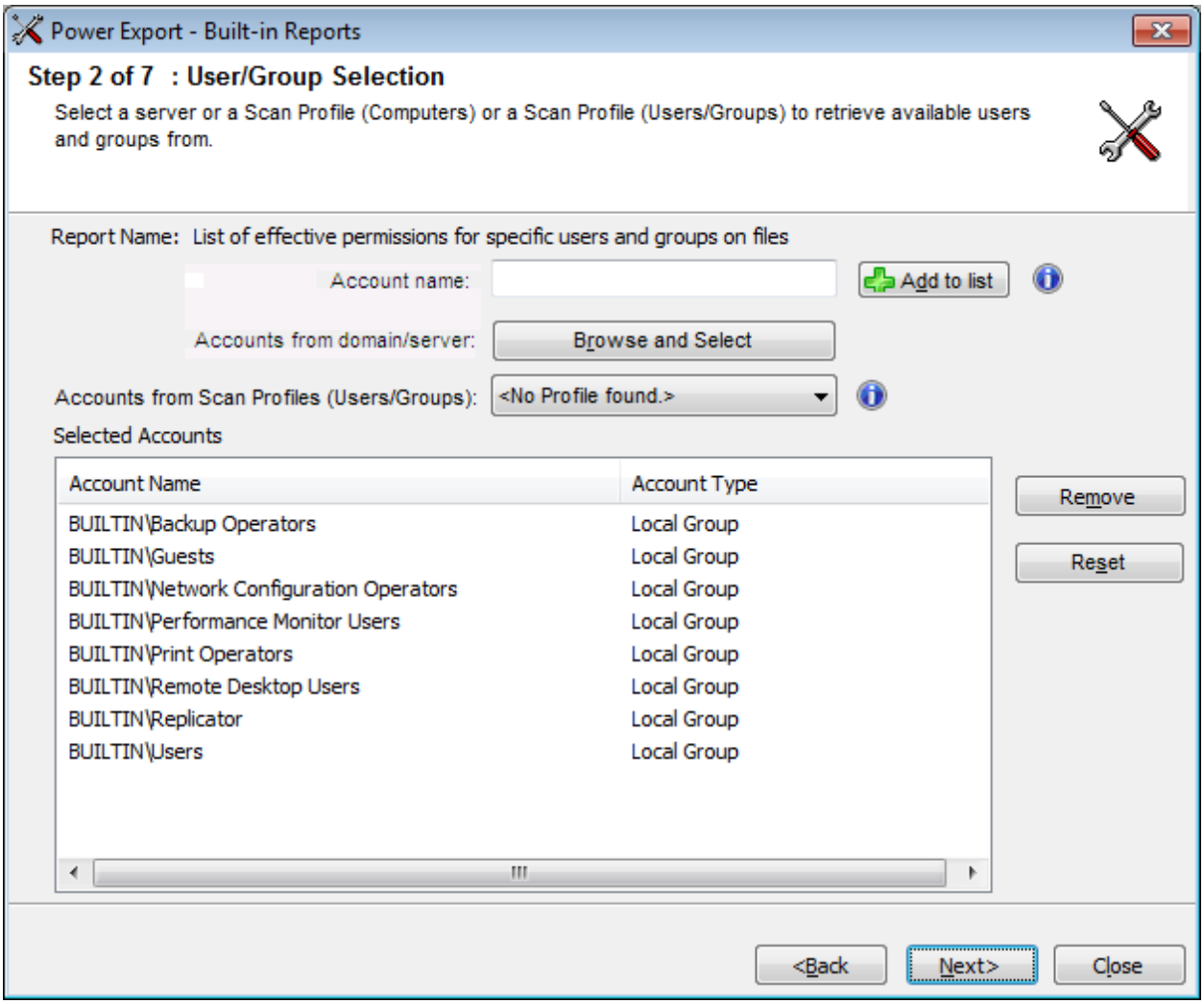
Step 1: Report Selection


Power Export - Built-in Reports
Step 1 of 6 : Report Selection
Select the desired report to proceed. Only one report can be selected in this category.
List of permissions for specific users and groups on folders
List of permissions for folders
List of permissions for specific users and groups on files
List of permissions for files
List of all permissions for folders (Inherited & Explicit)
List of effective permissions for users and groups on folders
List of effective permissions for users and groups on files
List of effective permissions for specific users and groups on folders
List of effective permissions for specific users and groups on files
<Back
Next>
Close

1. Select "**Permissions Reports**" from the select report category drop-down list.
2. Select the desired report. Only one report may be selected to run in a single task.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: User and/or Group Selection

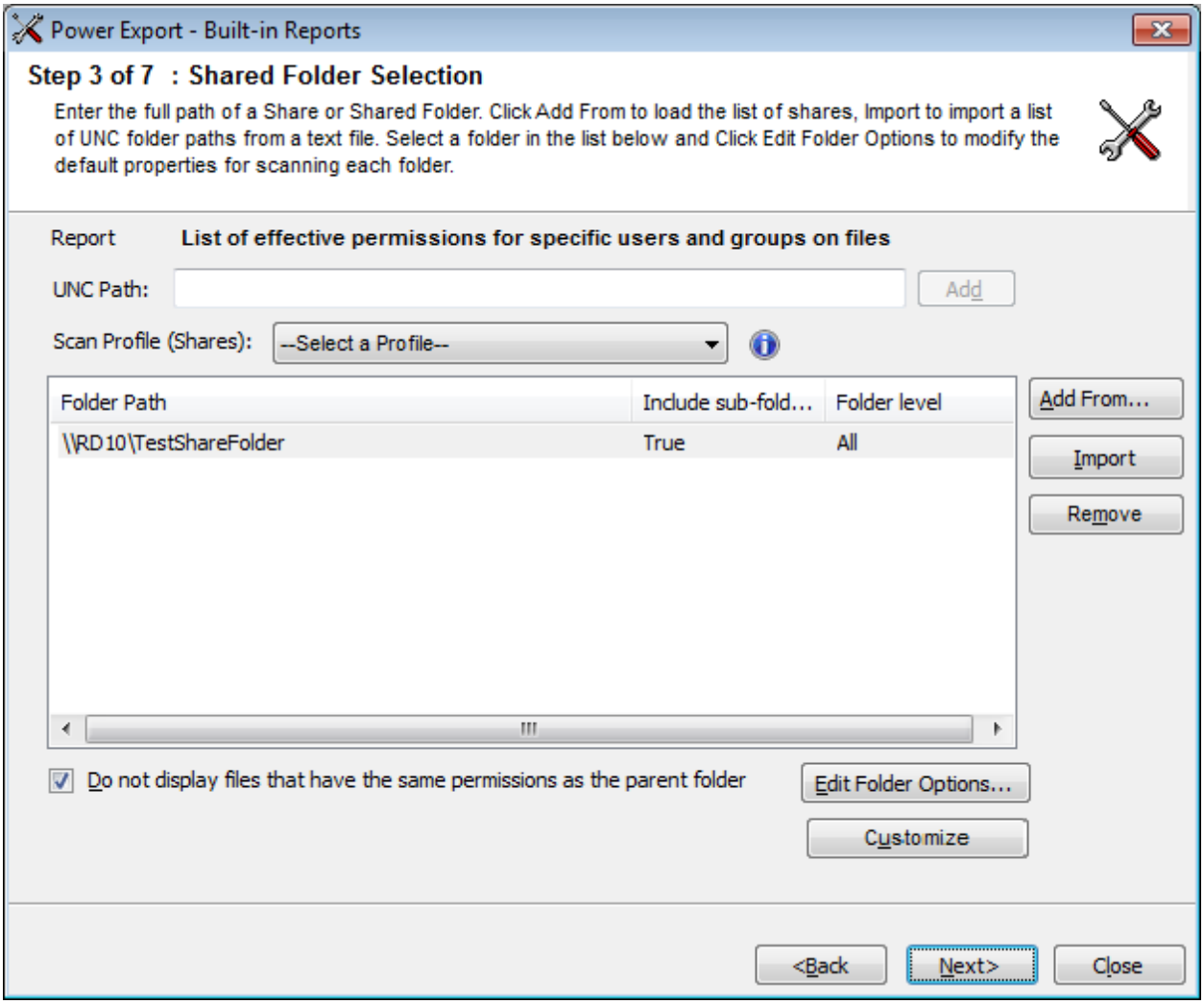

Power Export - Built-in Reports
Step 2 of 7 : User/Group Selection
Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.
Report Name: List of effective permissions for specific users and groups on files
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
<No Profile found.>
Selected Accounts
Account Name
Account Type
Remove
Reset
<Back
Next>
Close



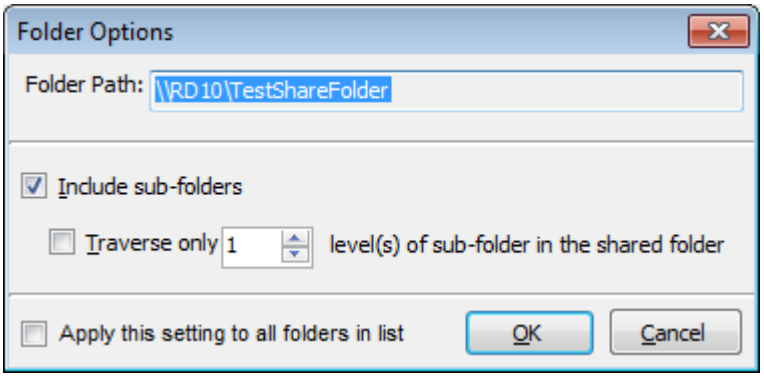
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).

1. Select the user or group, for which you wish to run the permissions report.
2. The selected users will be added to the wizard as shown above:
3. Click **Next** to proceed to the Next step.

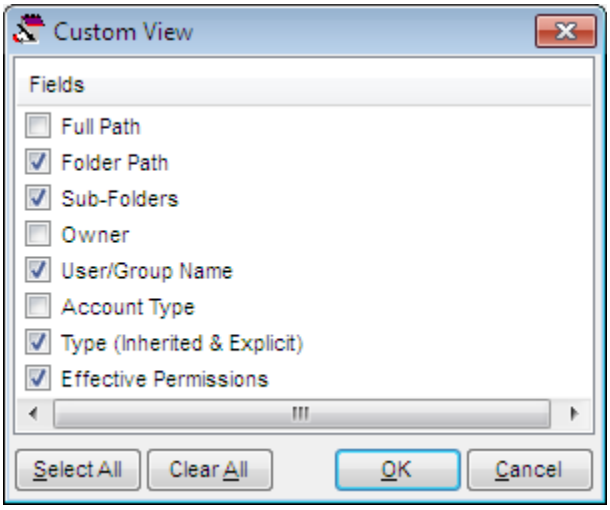
Step 3: Shared Folder Selection


Power Export - Built-in Reports
Step 3 of 7 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of effective permissions for specific users and groups on files
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
\\RD10\TestShareFolder
True
All
Add From...
Import
Remove
Do not display files that have the same permissions as the parent folder
Edit Folder Options...
Customize
<Back
Next>
Close

1. Select the desired folder(s) for which you wish to run the permissions report.
2. You may also click **Import** button to import a list of UNC folder paths from a text file.
3. Files that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want files with identical permissions as the parent folder reported, then select **Do not display files that have same permissions as the parent folder option**. This option will not report files with identical permissions as the parent folder.
4. NTFS Security Auditor defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:

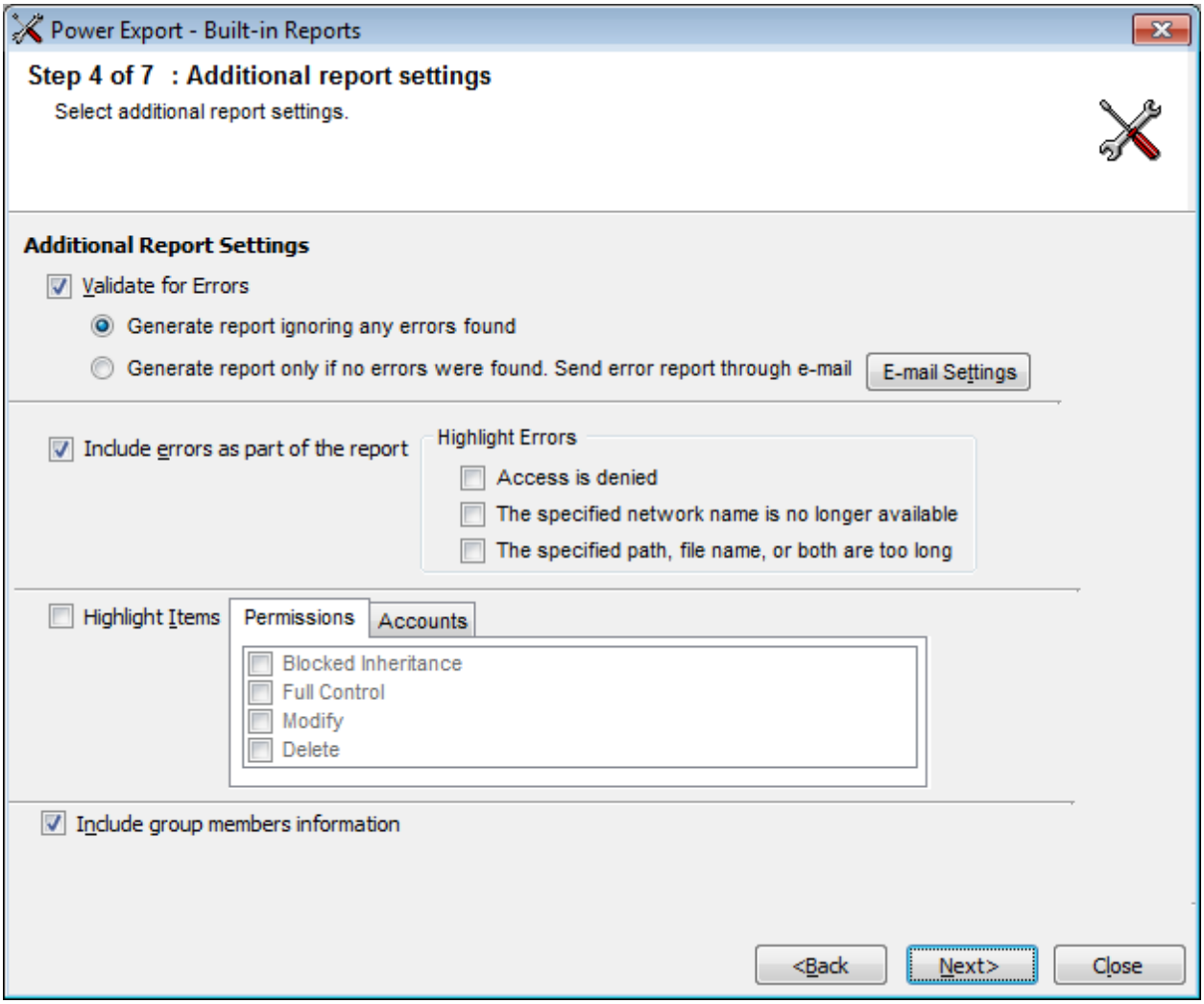


5. Modify the folder options as required and click **OK**.
6. You can use **Customize** option to exclude some of the fields from the report, as displayed below:



7. Select the customize options as required and click **OK**.
8. Click **Next** to proceed to the Next step.

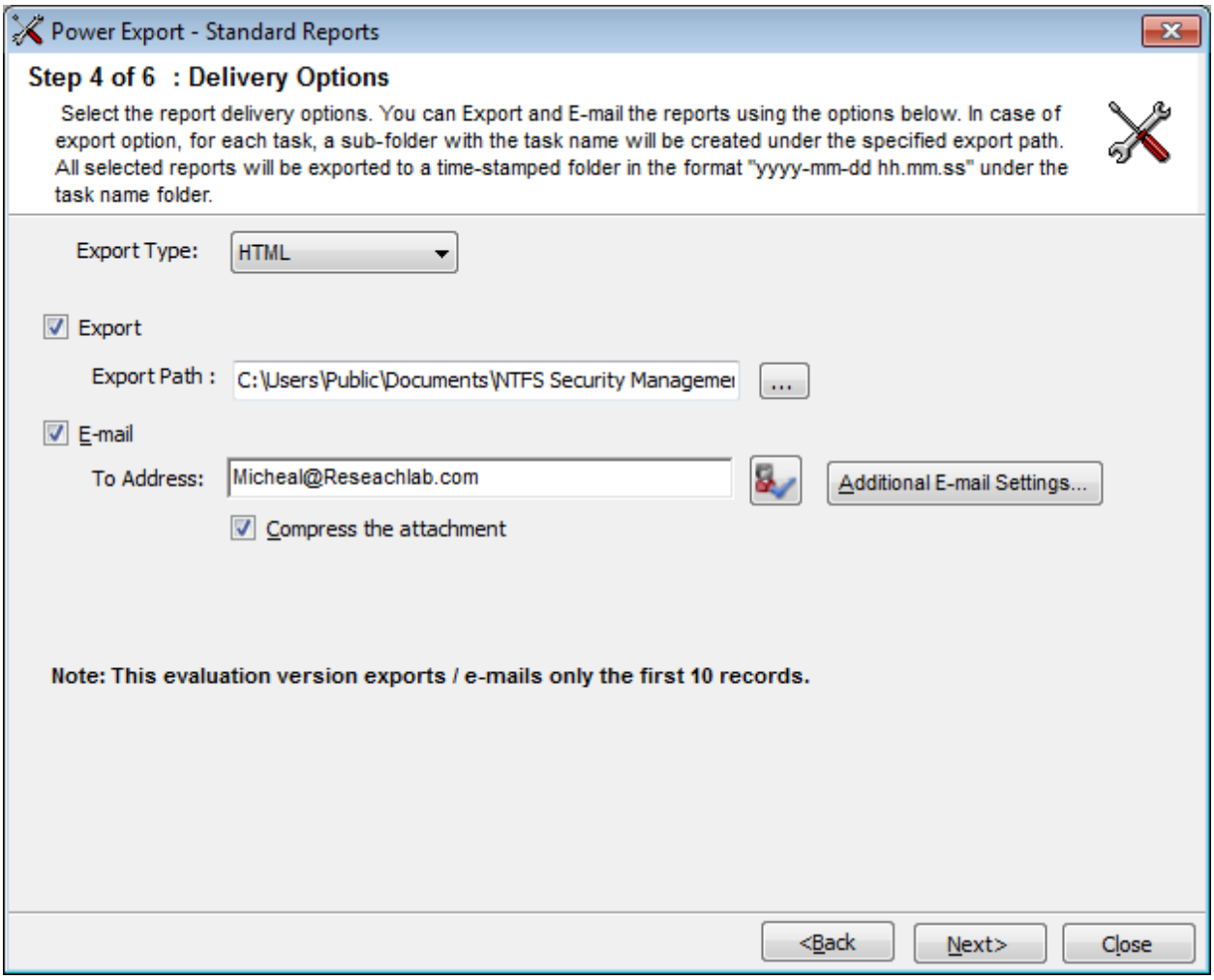
Step 4: Additional report settings


Power Export - Built-in Reports
Step 4 of 7 : Additional report settings
Select additional report settings.
Additional Report Settings
Validate for Errors
Generate report ignoring any errors found
Generate report only if no errors were found. Send error report through e-mail
E-mail Settings
Include errors as part of the report
Highlight Errors
Access is denied
The specified network name is no longer available
The specified path, file name, or both are too long
Highlight Items
Permissions
Accounts
Blocked Inheritance
Full Control
Modify
Delete
Include group members information
<Back
Next>
Close

1. Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
   - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
   - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
2. You may select **Include errors as part of the report** option for including the error information of folders / files into report data. Select error information that needs to be highlighted.
3. You may also select **Highlight Items** for highlighting rows containing certain Permissions and Account status in the report data. Select the desired Permissions and status of Accounts that need to be highlighted.

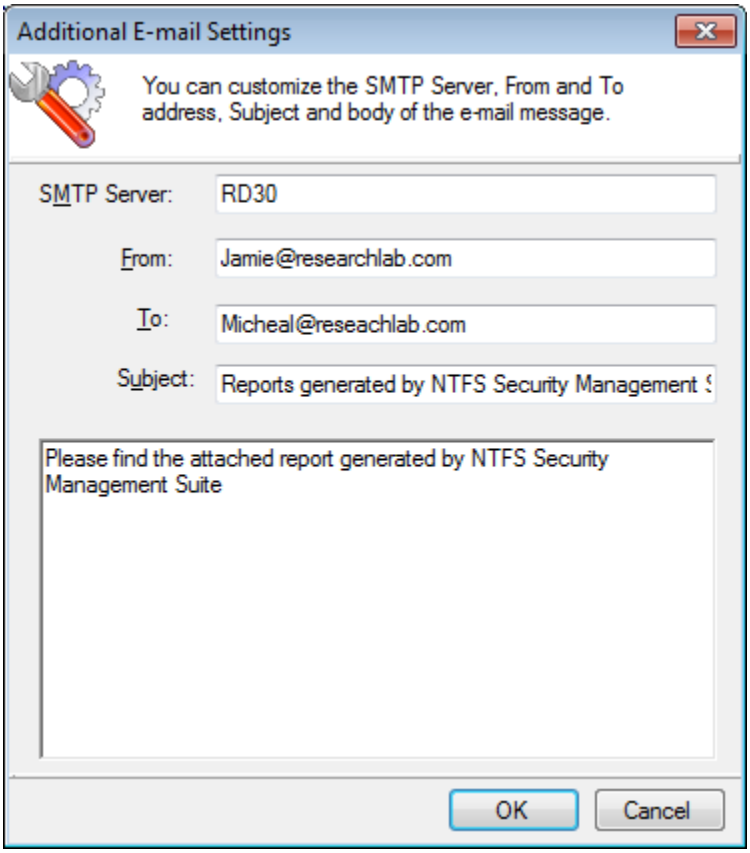
4. You may also select **Include group members information** for include members of a group and their sub-group members at all group levels in the report.
5. Click **Next** to proceed to the Next step.

Step 5: Delivery Options

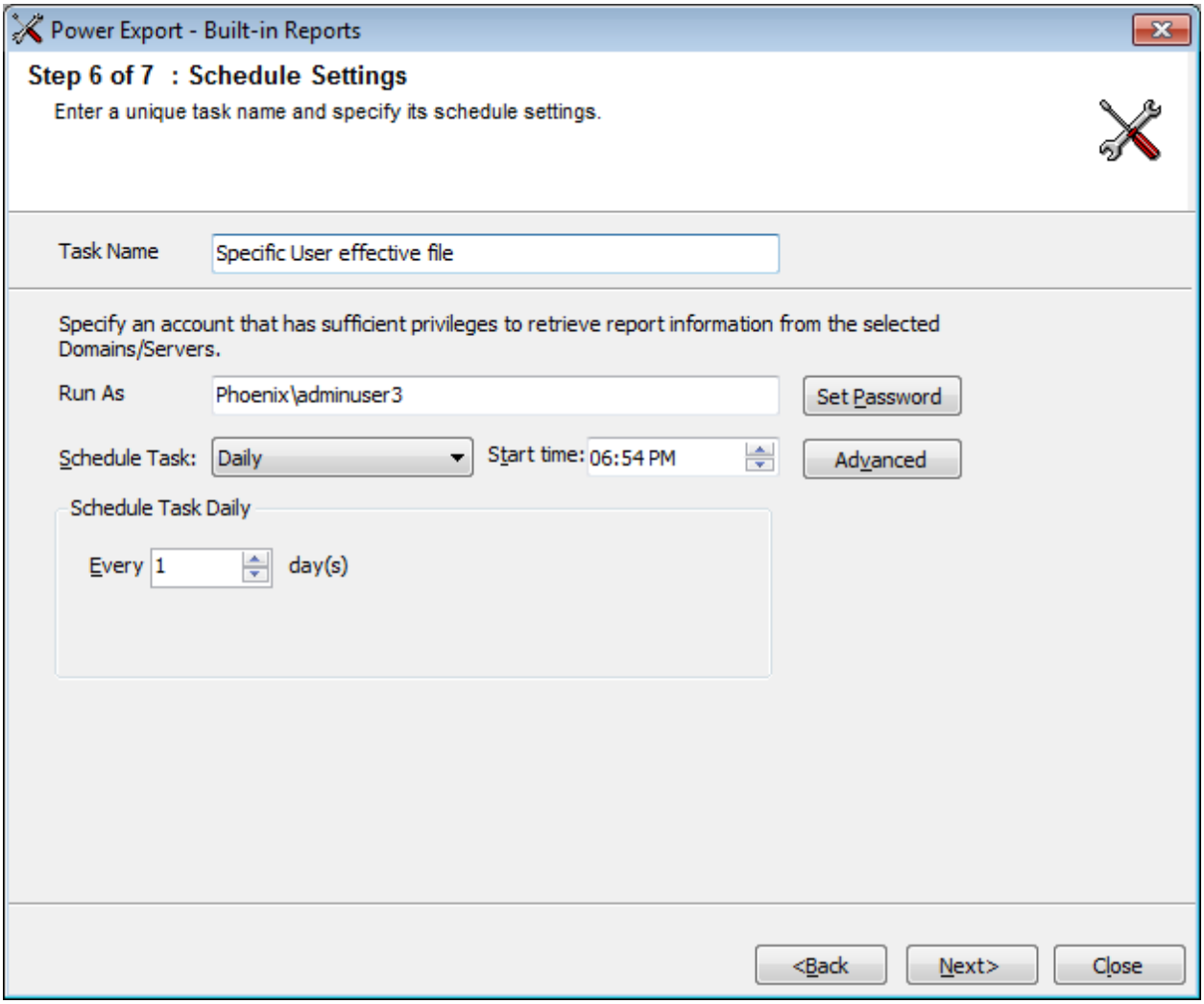

Power Export - Standard Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Micheal@Reseachlab.com
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.

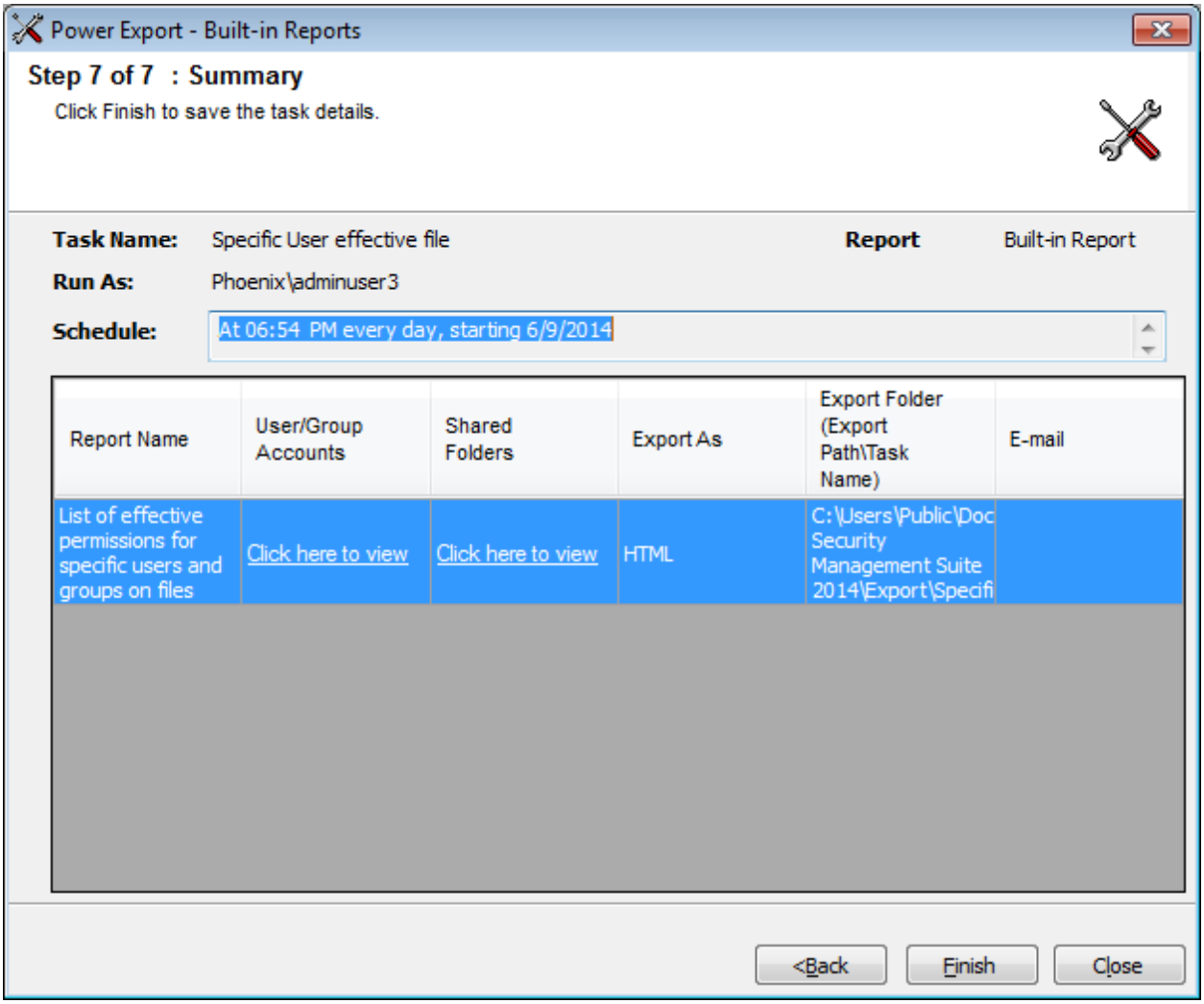

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 6: Schedule Settings



1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 7: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Scheduled Tasks folder.

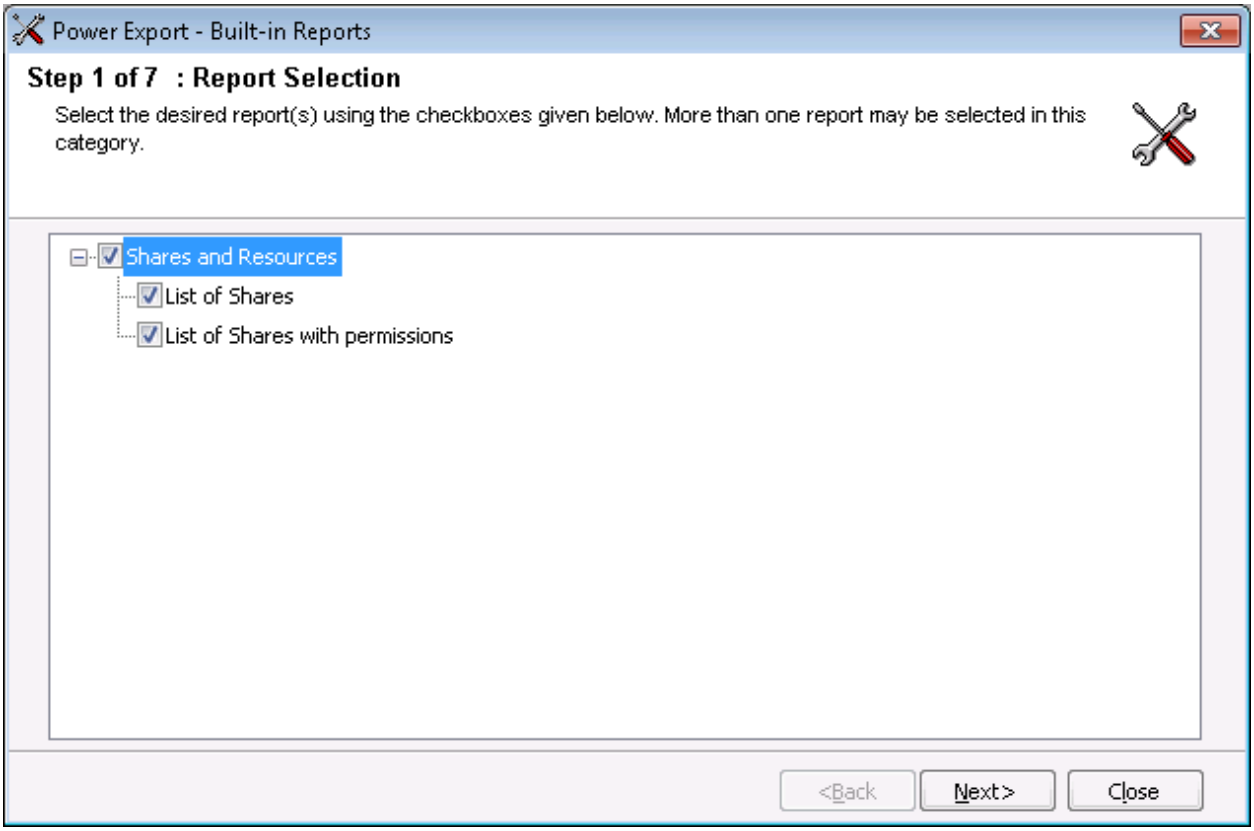
Schedule Shares and Resources Built-in Reports

Click

option under Power Export.

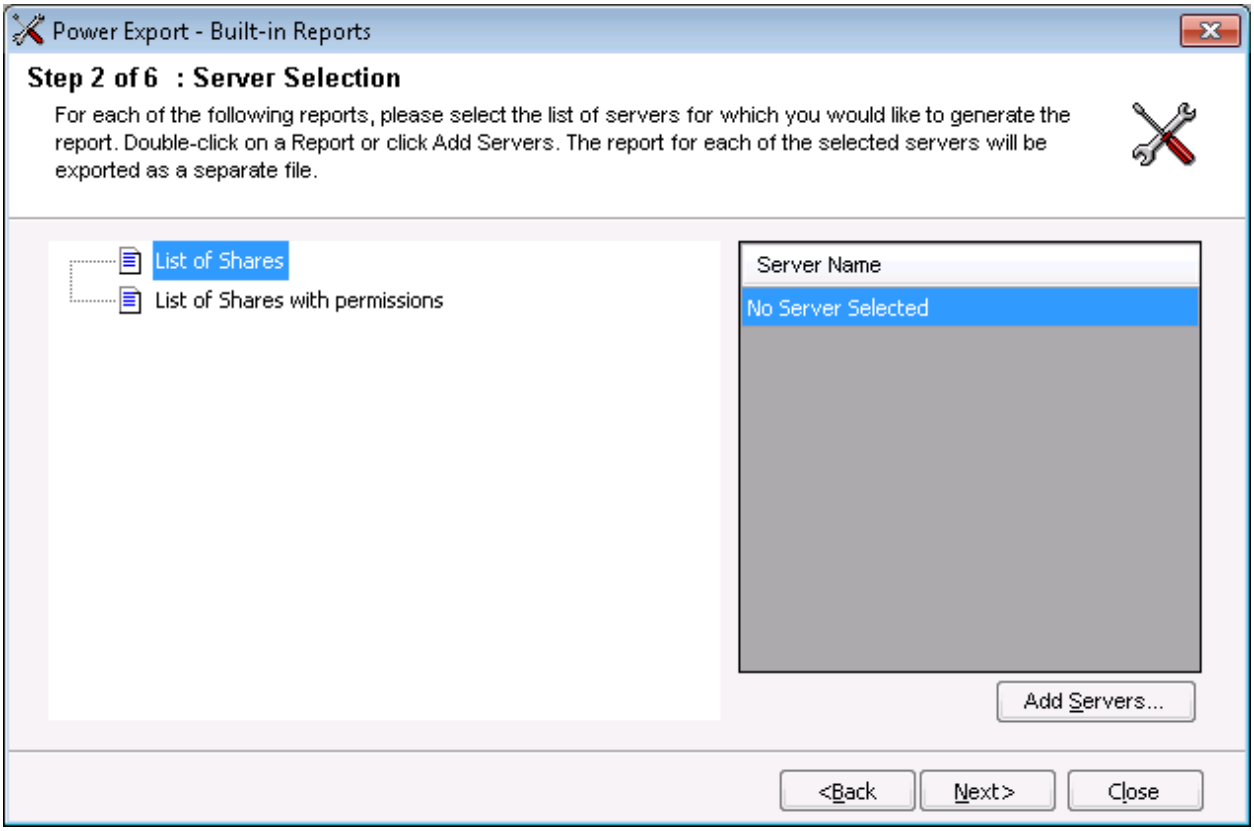
This will bring up the Power Export Wizard.

Step 1: Report Selection

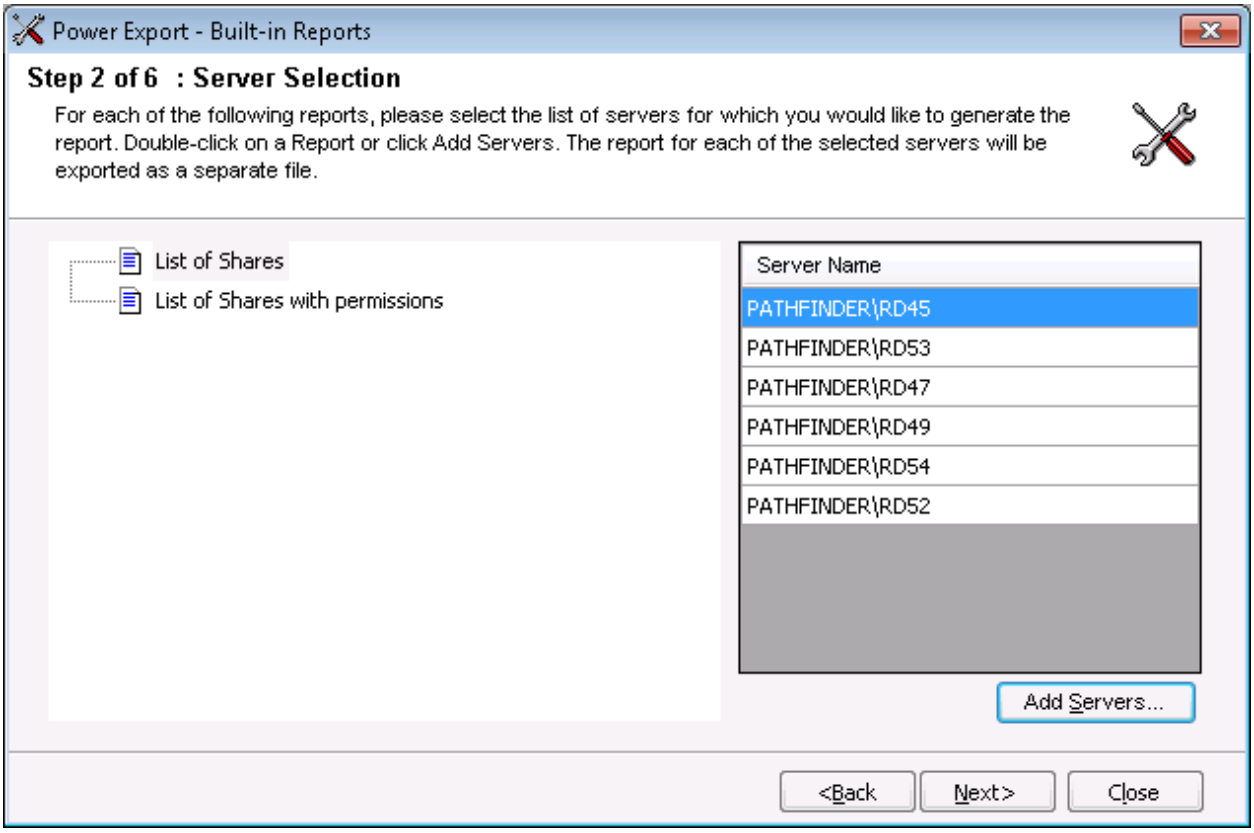

Power Export - Built-in Reports
Step 1 of 7 : Report Selection
Select the desired report(s) using the checkboxes given below. More than one report may be selected in this category.
Shares and Resources
List of Shares
List of Shares with permissions
<Back
Next>
Close

1. Select the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
2. The above reports collect data on a server-basis.
3. Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: Server Selection

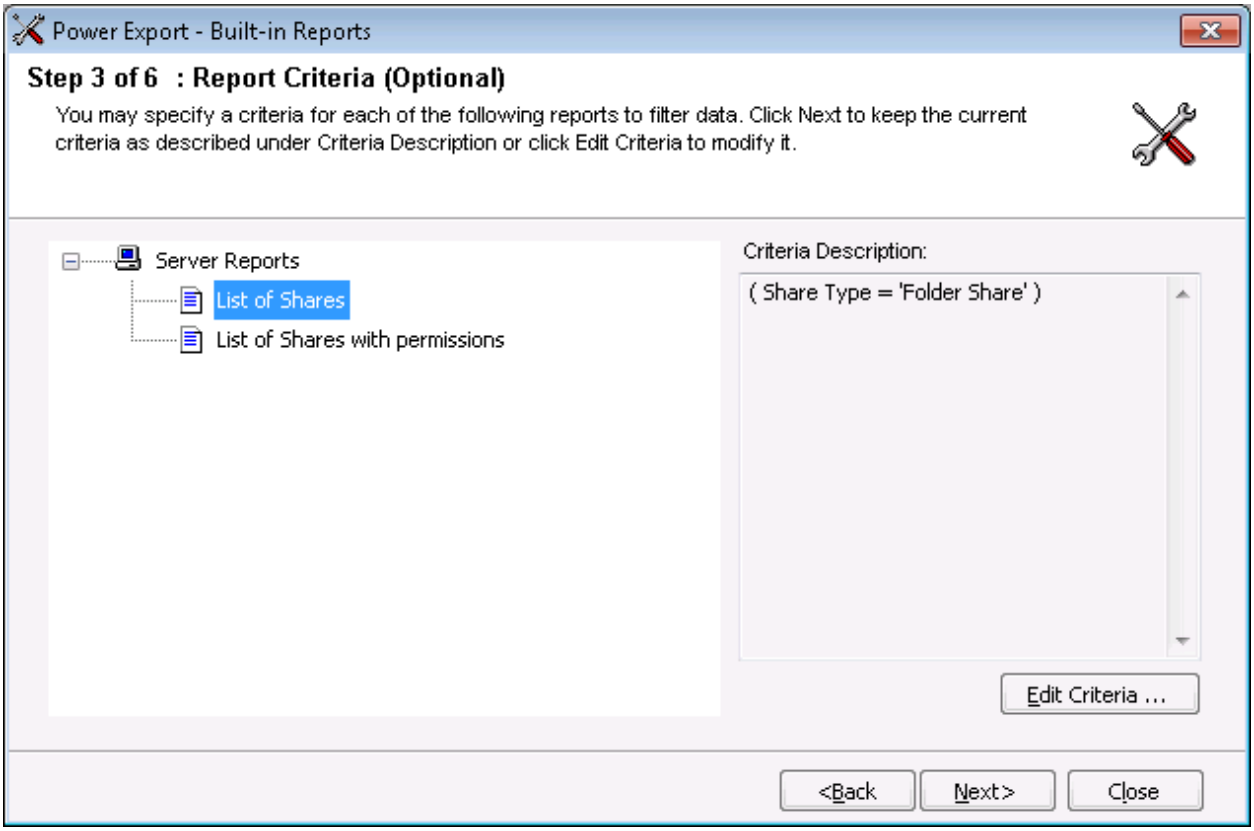

Power Export - Built-in Reports
Step 2 of 6 : Server Selection
For each of the following reports, please select the list of servers for which you would like to generate the report. Double-click on a Report or click Add Servers. The report for each of the selected servers will be exported as a separate file.
List of Shares
List of Shares with permissions
Server Name
No Server Selected
Add Servers...
<Back
Next>
Close

1. Click **Add Servers** button to select the servers for which you wish to run the server reports selected in Step 1. This will display a window where you can select the servers you want to add. Selecting a domain will add all the servers in that domain to the report.
2. Click **OK** to apply the selected servers to the current report or click **Apply to Reports** to apply the servers to the rest of the selected server reports. The selected servers will be added to the wizard as shown below:


Power Export - Built-in Reports
Step 2 of 6 : Server Selection
For each of the following reports, please select the list of servers for which you would like to generate the report. Double-click on a Report or click Add Servers. The report for each of the selected servers will be exported as a separate file.
List of Shares
List of Shares with permissions
Server Name
PATHFINDER\RD45
PATHFINDER\RD53
PATHFINDER\RD47
PATHFINDER\RD49
PATHFINDER\RD54
PATHFINDER\RD52
Add Servers...
<Back
Next>
Close

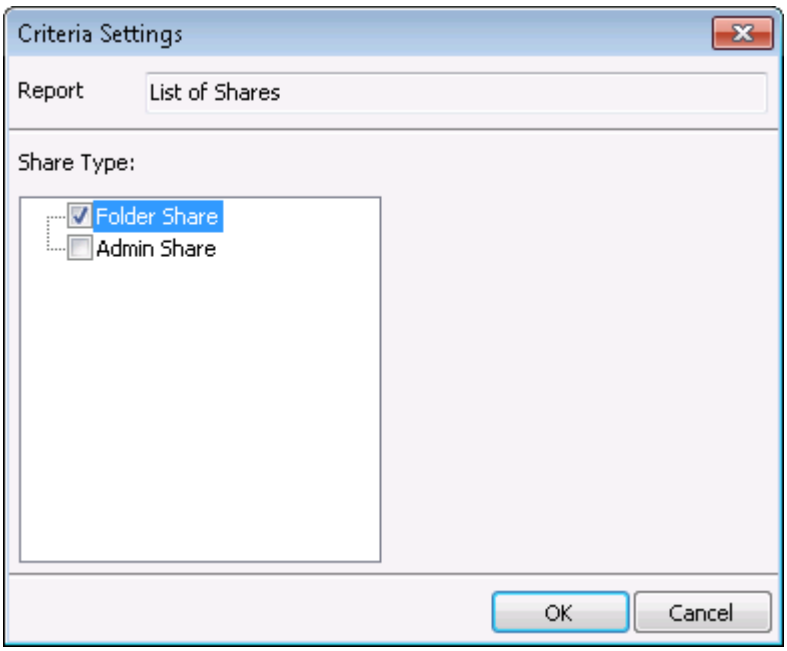
3. Click **Next** to proceed to the next Step.

Step 3: Report Criteria (Optional)

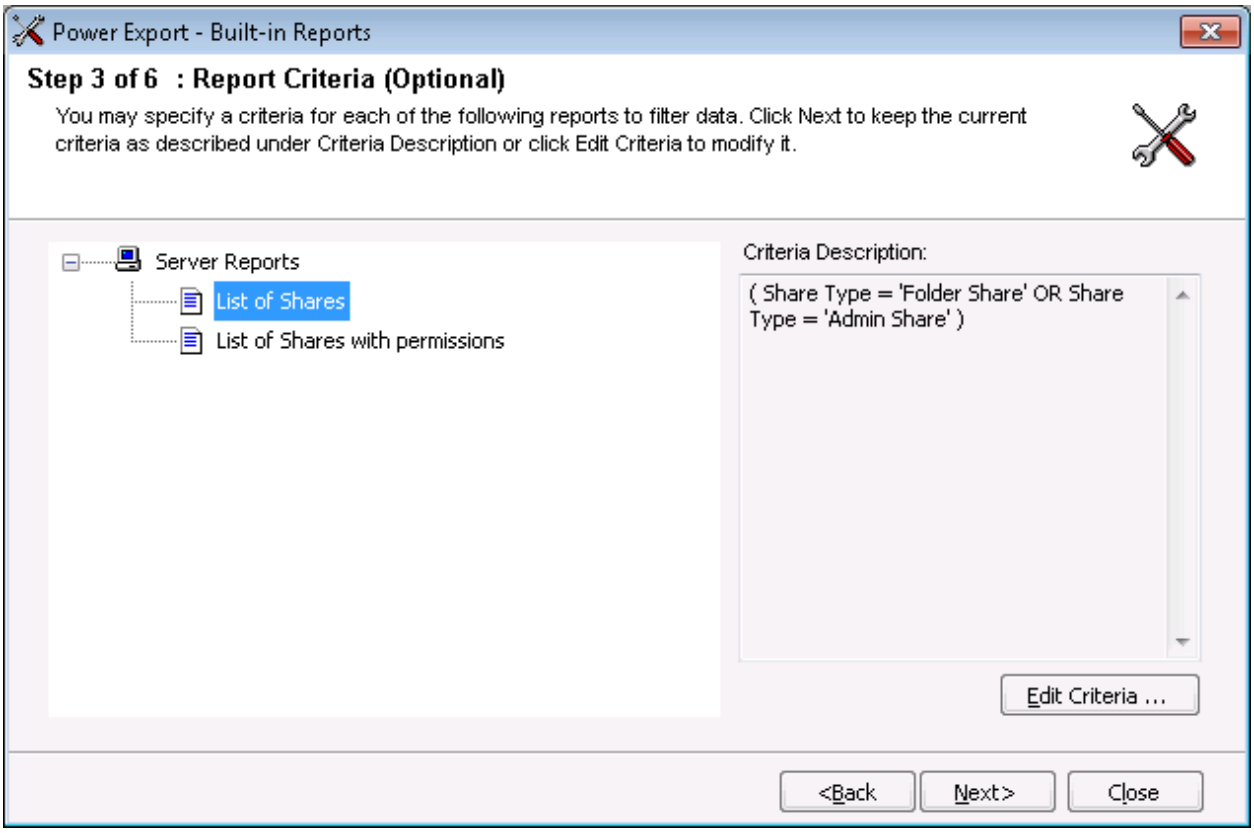

Power Export - Built-in Reports
Step 3 of 6 : Report Criteria (Optional)
You may specify a criteria for each of the following reports to filter data. Click Next to keep the current criteria as described under Criteria Description or click Edit Criteria to modify it.
Server Reports
List of Shares
List of Shares with permissions
Criteria Description:
(Share Type = 'Folder Share')
Edit Criteria ...
<Back
Next>
Close

This step allows you to apply specific conditions for filtering report data.

1. To set a criteria for a report, select a report and Click **Edit Criteria** or Double Click the report.
2. The Criteria Settings window will be displayed as shown below:

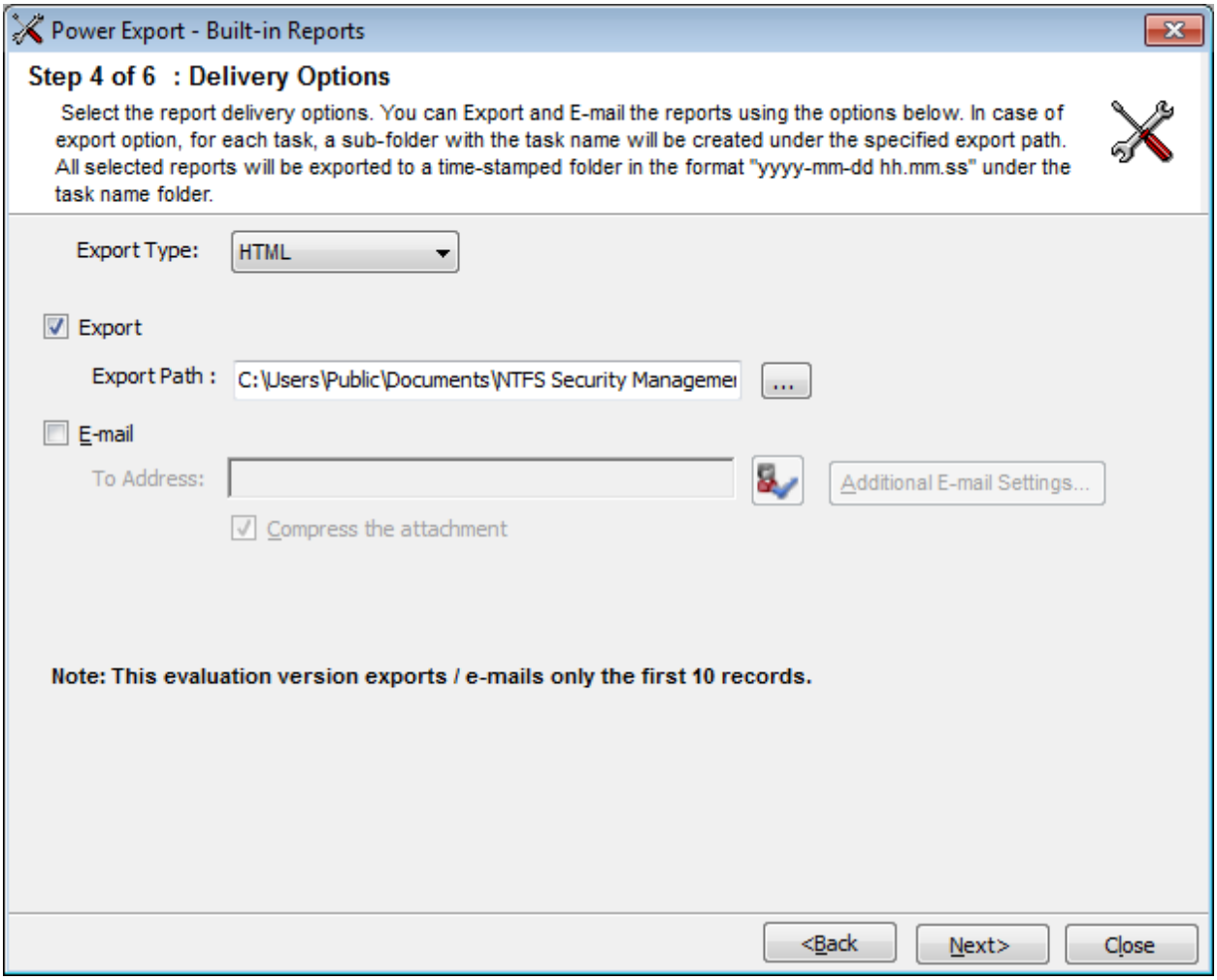


3. Specify the criteria to filter the report data using the checkboxes.
4. Click **OK** in Criteria Settings window to go back to the wizard.
5. A description of the selected criteria will be displayed under Criteria Description as shown below:


Power Export - Built-in Reports
Step 3 of 6 : Report Criteria (Optional)
You may specify a criteria for each of the following reports to filter data. Click Next to keep the current criteria as described under Criteria Description or click Edit Criteria to modify it.
Server Reports
List of Shares
List of Shares with permissions
Criteria Description:
(Share Type = 'Folder Share' OR Share Type = 'Admin Share')
Edit Criteria ...
<Back
Next>
Close

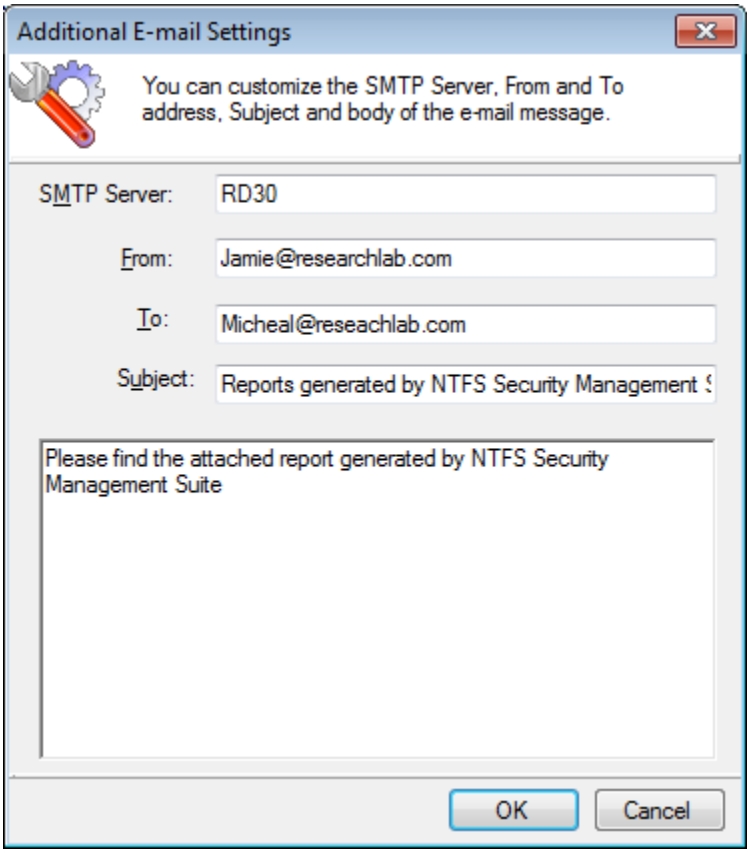
6. Click **Next** to proceed to the Next step.

Step 4: Delivery Options

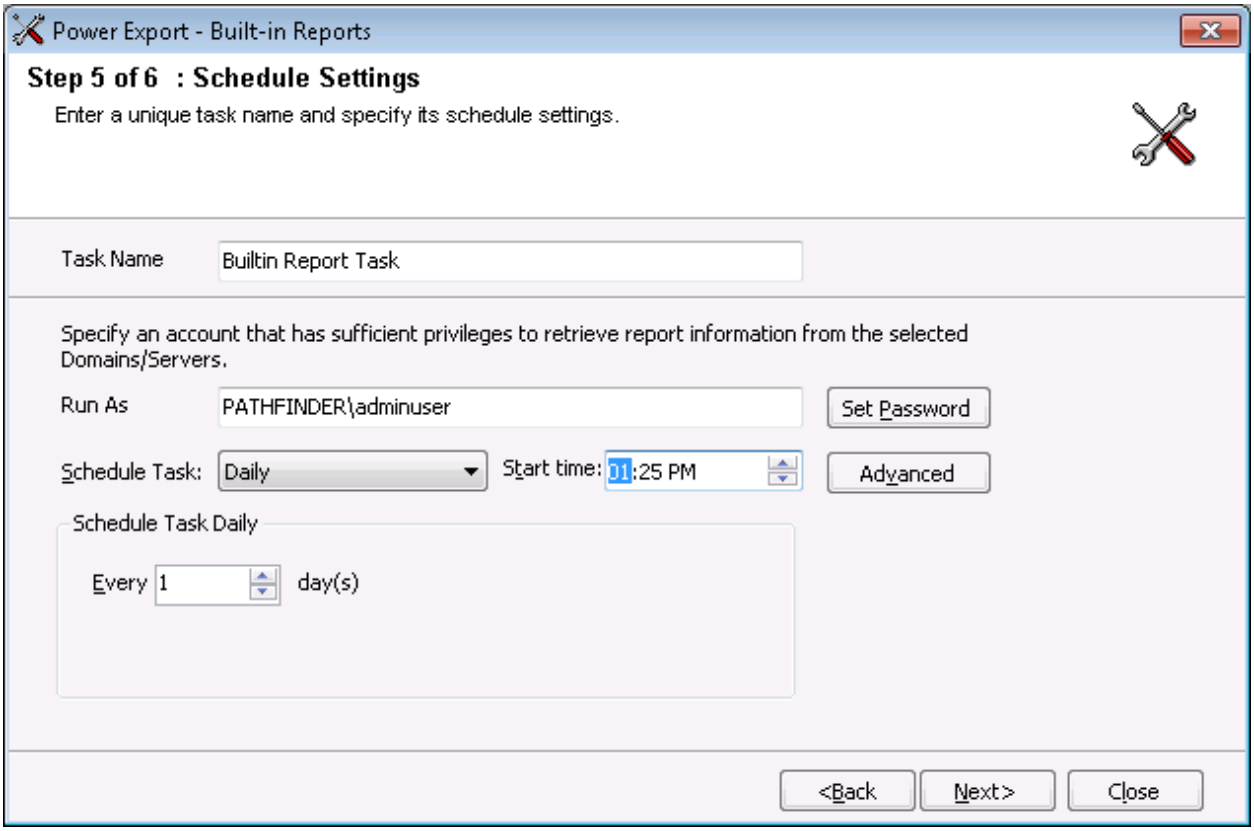

Power Export - Built-in Reports
Step 4 of 6 : Delivery Options
Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.
Export Type:
HTML
Export
Export Path :
C:\Users\Public\Documents\NTFS Security Manageme
...
E-mail
To Address:
Additional E-mail Settings...
Compress the attachment
Note: This evaluation version exports / e-mails only the first 10 records.
<Back
Next>
Close

1. Change the Export or E-mail settings as necessary.
2. Use Browse button to change the export path.
3. Click Next to proceed to the next step.

- Click Additional E-mail Settings button to specify optional e-mail settings as shown below

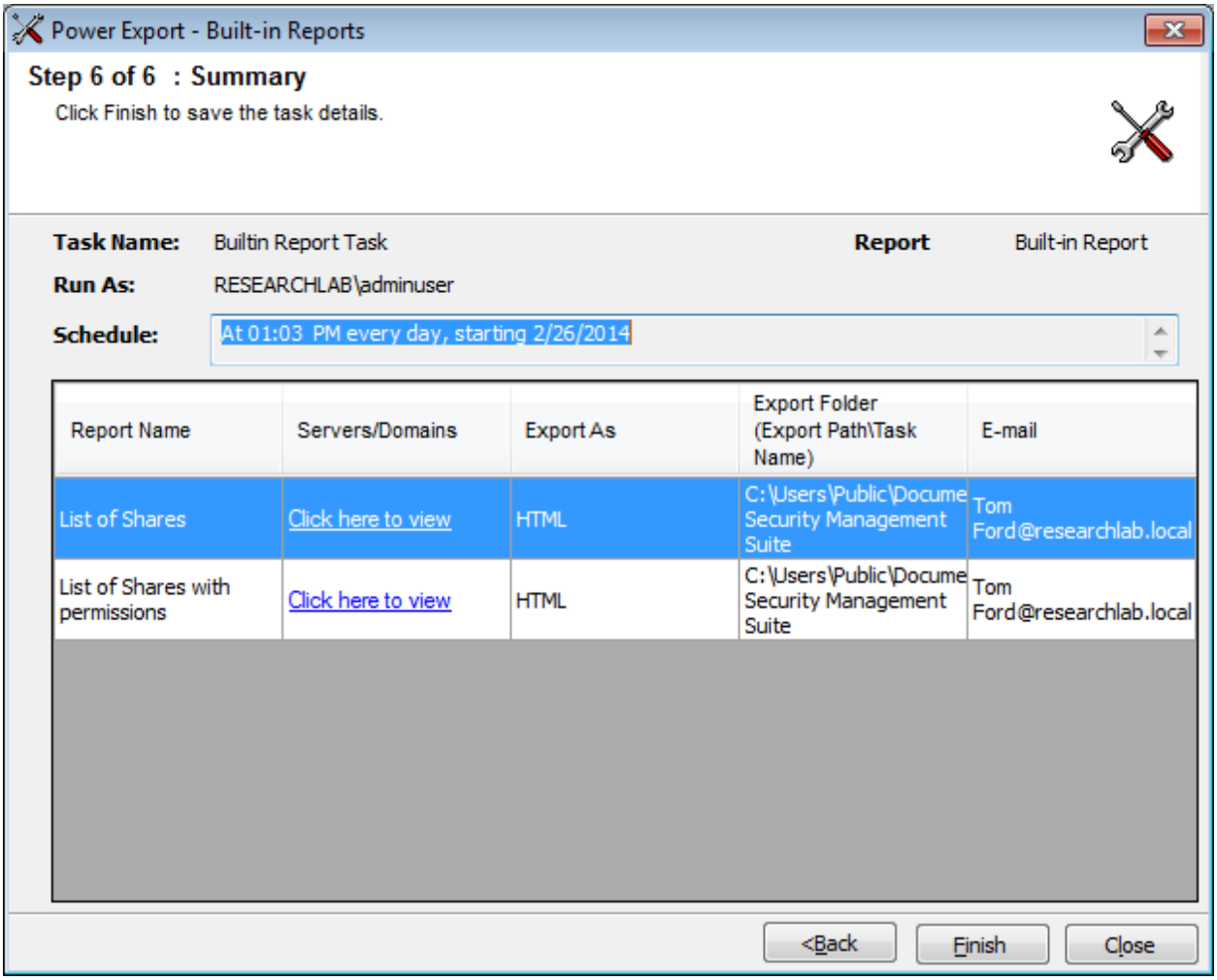

Additional E-mail Settings
You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.
SMTP Server:
RD30
From:
Jamie@researchlab.com
To:
Micheal@reseachlab.com
Subject:
Reports generated by NTFS Security Management
Please find the attached report generated by NTFS Security Management Suite
OK
Cancel

Step 5: Schedule Settings

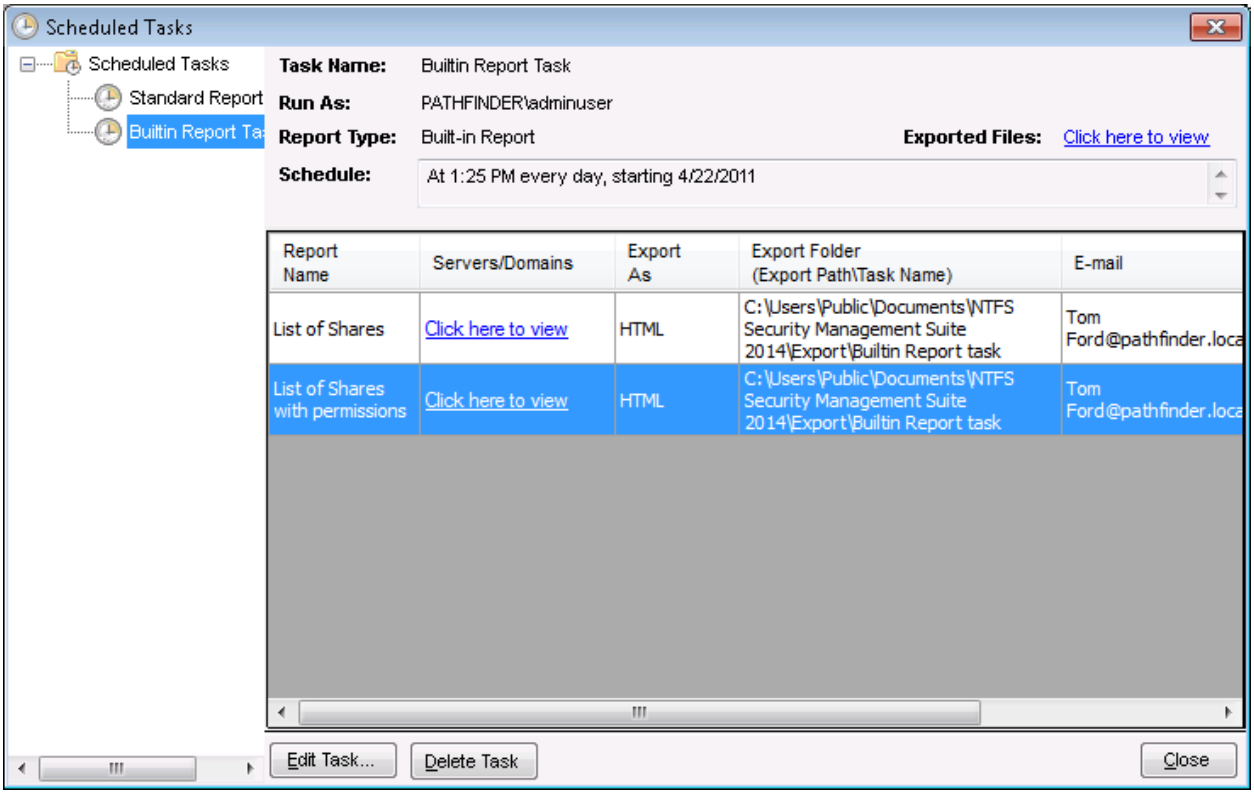


1. Enter a unique name for the task.
2. Change the Run as parameter, if necessary and set the password for the specified user.
3. Change the task schedule settings as required.
4. Click **Next** to proceed to the next and final step.

Step 6: Summary



1. This step displays the summary information of the task.
2. Click **Finish** to save the task details.
3. The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:


Scheduled Tasks
Scheduled Tasks
Standard Report
Builtin Report Ta
Task Name: Builtin Report Task
Run As: PATHFINDER\adminuser
Report Type: Built-in Report
Exported Files: Click here to view
Schedule: At 1:25 PM every day, starting 4/22/2011
Report Name
Servers/Domains
Export As
Export Folder (Export Path\Task Name)
E-mail
List of Shares
Click here to view
HTML
C:\Users\Public\Documents\NTFS Security Management Suite 2014\Export\Builtin Report task
Tom Ford@pathfinder.loca
List of Shares with permissions
Click here to view
HTML
C:\Users\Public\Documents\NTFS Security Management Suite 2014\Export\Builtin Report task
Tom Ford@pathfinder.loca
Edit Task...
Delete Task
Close

NTFS Security Manager

Grant Permissions

Revoke Permissions

Modify Permissions

Copy Permissions

Dynamic Access Control

Power Search

Change History

Grant Permissions

About Grant Permissions

How to Grant Permissions for selected Shares?

How to reuse the Grant Permissions templates?

About Grant Permissions

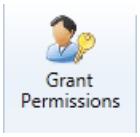
The **Grant Permissions** feature allows you to grant permissions to the Share permissions. You can use many options like Add the new permissions to the account's existing permissions, Replace the account's existing permissions with the new permissions, etc. You may select options to Allow, Block inheritance from the parent object and also Replace all child objects existing permissions with the inheritable permissions from this object while granting permissions for accounts. Here is the list of actions you can perform using the Grant Permissions feature.

Note: This feature will not break the inheritance from the parent of current object. If you still wish to break the inheritance from the parent object, you may use the option "Block Inherited permissions from this object's parent" to block inheritance.

Actions
Grant permissions for selected Shares: (How to?)
Grant permissions for the selected accounts to the selected shared folder(s)/file(s) permissions list.
Replace existing accounts permissions with the new permissions: (How to?)
Replace the existing accounts permissions, If an existing account is selected to grant permissions to a shared folder.
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files): (How to?)
Grant permissions on subfolders and files that do not have inherited permissions from its parent object with respect to the above options.
Remove all the existing explicit accounts and replace with the new accounts: (How to?)
Remove all existing accounts that have explicitly assigned permissions for shares and replace them with the selected accounts and permissions.
Replace all explicit permissions existing in descendant with the inherited permissions from the current object: (How to?)
Remove explicitly defined permissions on all descendant objects and replace them with the inheritable permissions from the shared folder(s)/file(s) permissions list.
Allow inherited permissions from the parent object to the current shares: (How to?)
Allow inheritable permissions from the parent object to the current shares. It will not affect the already existing explicit permissions.
Copy and Remove inherited permissions from the parent object to the current shares: (How to?)
Copy and Remove the inheritable permissions from the parent object to the current shares. Copying the inheritable permissions will add the inherited permissions as explicit permissions in the shares permissions list. Removing the inherited permissions will remove all the inherited permissions from the parent to the current object.

How to replace existing accounts permissions with the new permissions?

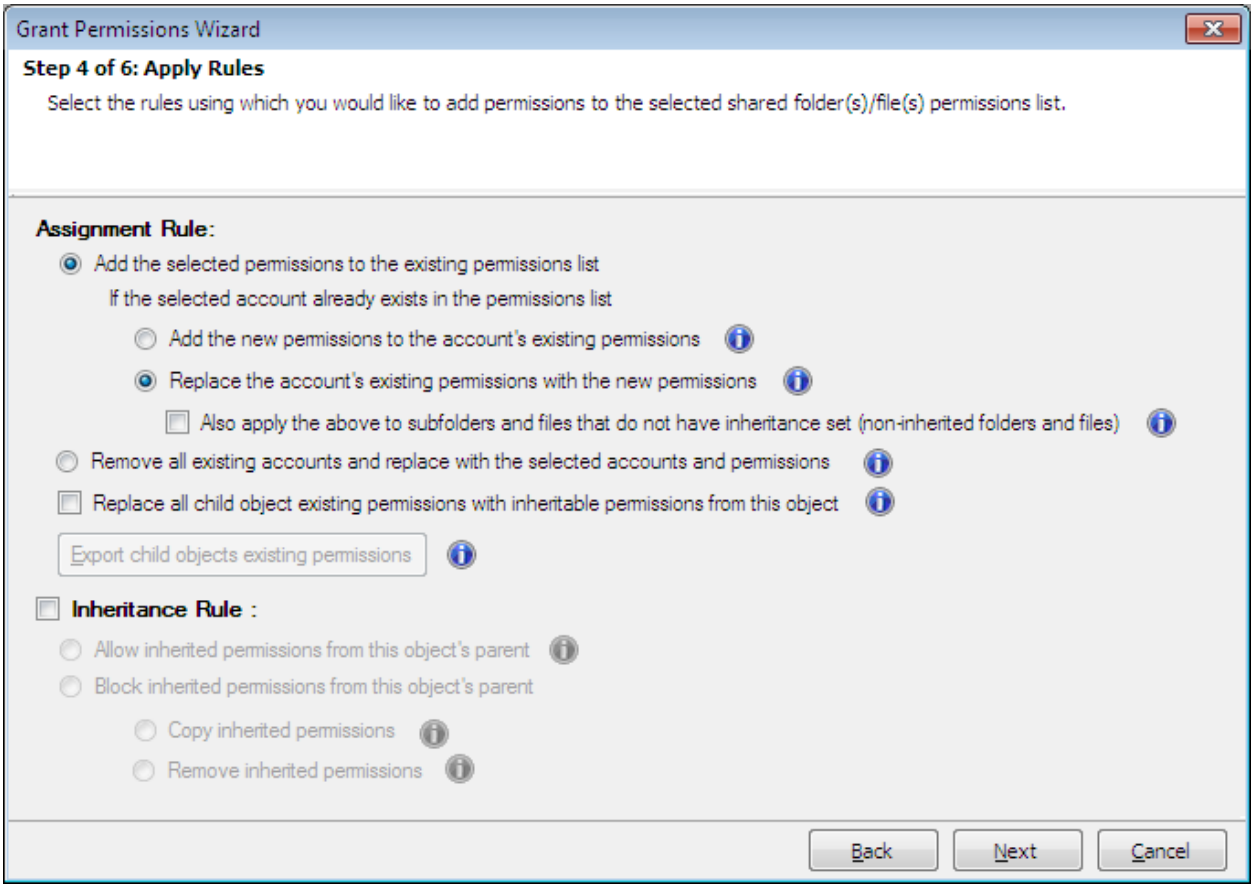
The Grant Permissions feature allows you to replace the existing accounts permissions, If the existing account selected for grant permissions.

Click on 

button.

The Grant Permissions window will be displayed.

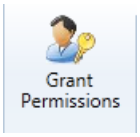
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?.
- In step 4 select the option Replace the account's existing permissions with the new permissions.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to grant permissions to the selected accounts on subfolders and files that do not have inherited permissions from its parent object?

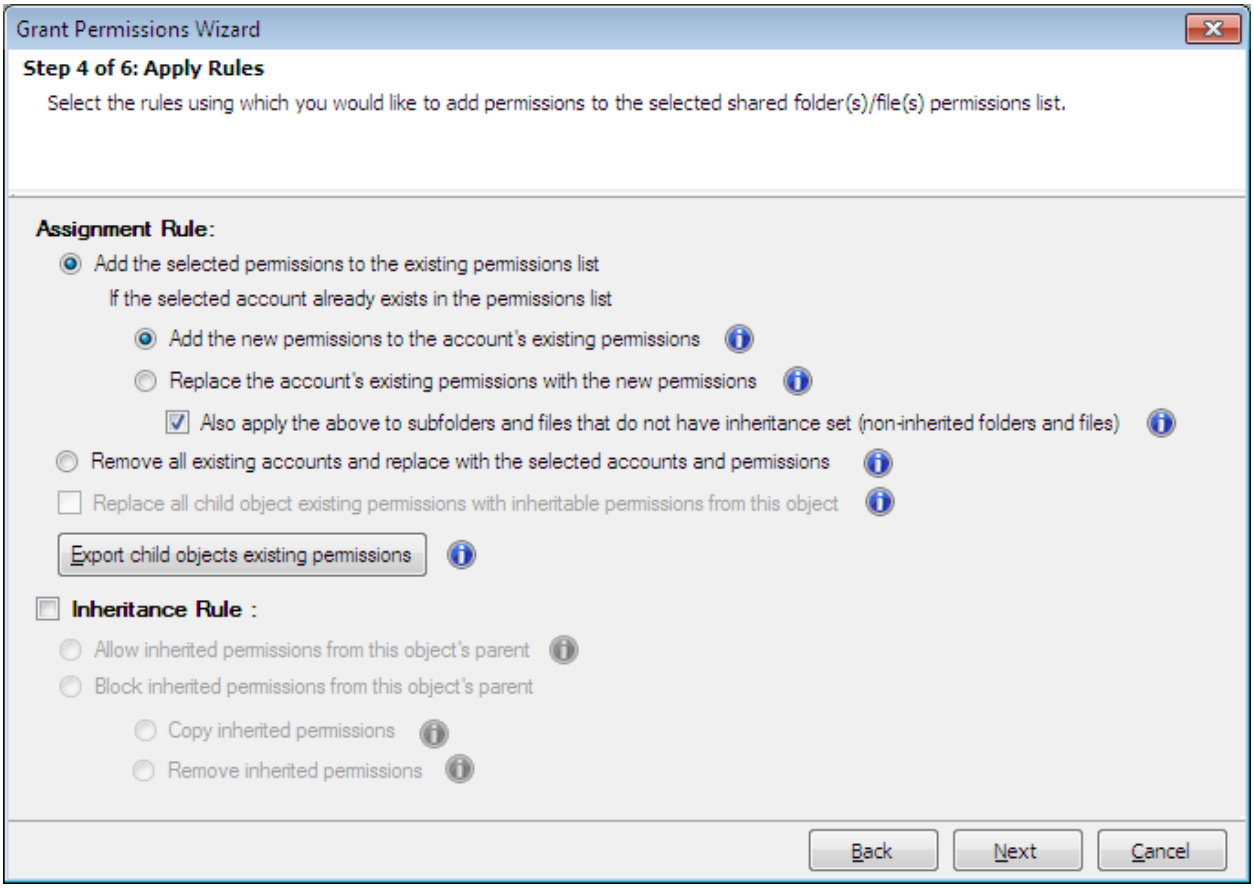
The Grant Permissions feature allows to grant permissions to the selected accounts on all subfolders and files that do not have inherited permissions from its parent object.

Click on 

button.

The Grant Permissions window will be displayed.

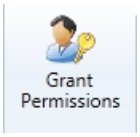
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?.
- In step 4 select the option "Add the new permissions to the account's existing permissions" or "Replace the account's existing permissions with the new permissions"
- Then select the option Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files).


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to remove all the existing explicit accounts and replace with the new accounts?

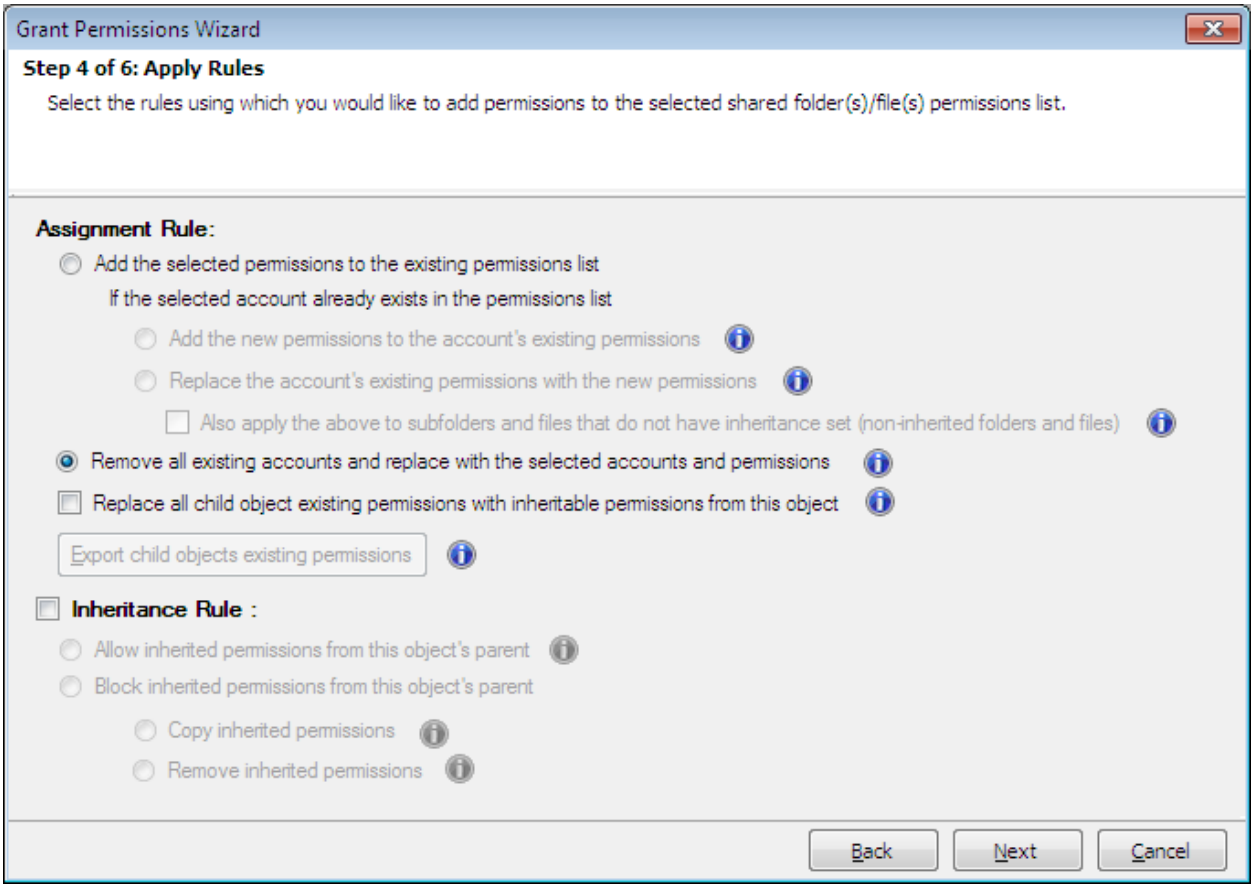
The Grant Permissions feature allows you to remove all existing accounts that have explicitly assigned permissions for shares and replace them with the selected accounts and permissions. Note that this will not remove inherited permissions from parent folder.

Click on 

button.

The Grant Permissions window will be displayed.

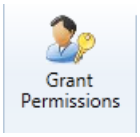
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?
- In step 4 select the option Remove all existing accounts and replace with the selected accounts and permissions.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to replace all explicit permissions existing in descendant with the inherited permissions from the current object?

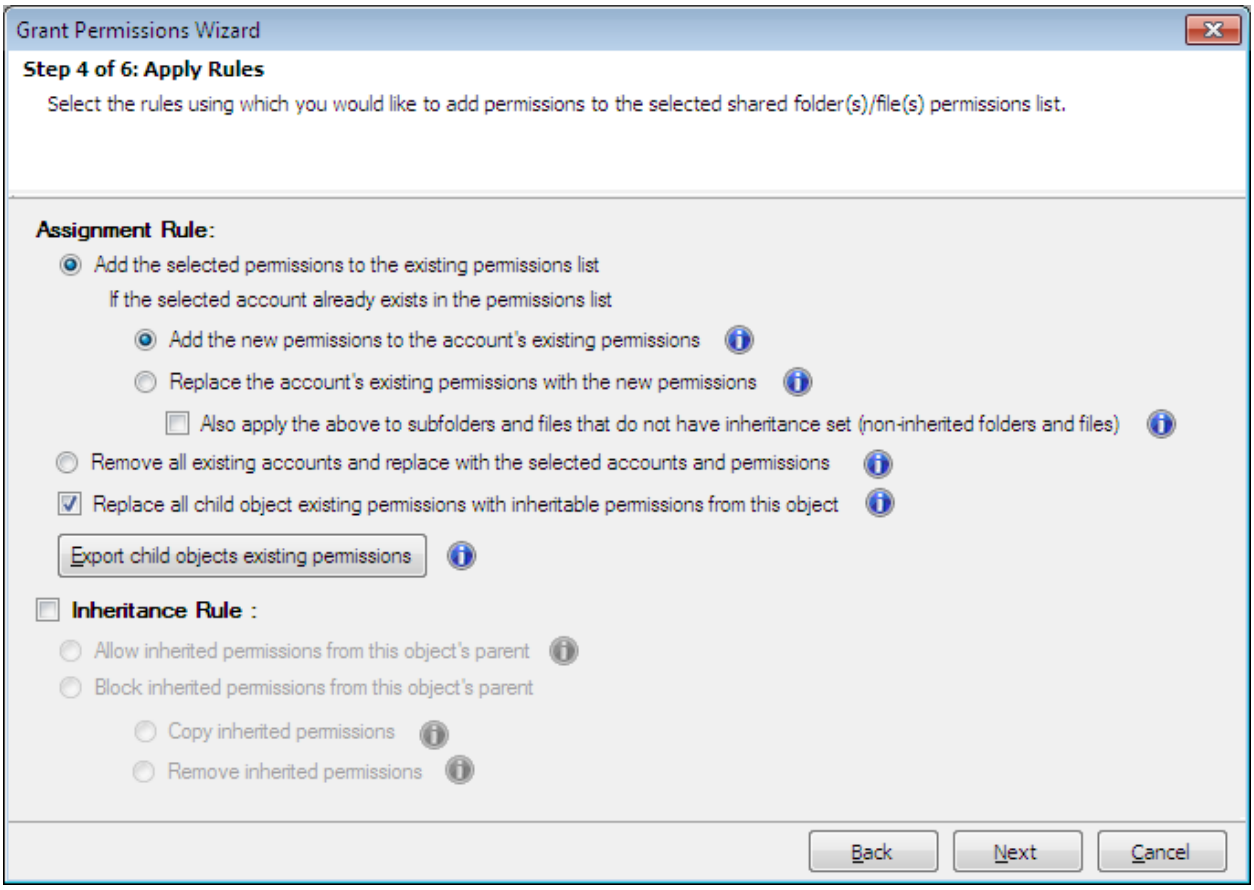
The Grant Permissions feature allows to remove explicitly defined permissions on all descendant object and replace them with the inheritable permissions from the shared folder(s)/file(s) permissions list.

Click on 

button.

The Grant Permissions window will be displayed.

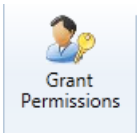
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?.
- In step 4 select the option Replace all child objects existing permissions with the inheritable permissions from this object.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to allow inherited permissions from the parent object to the current share?

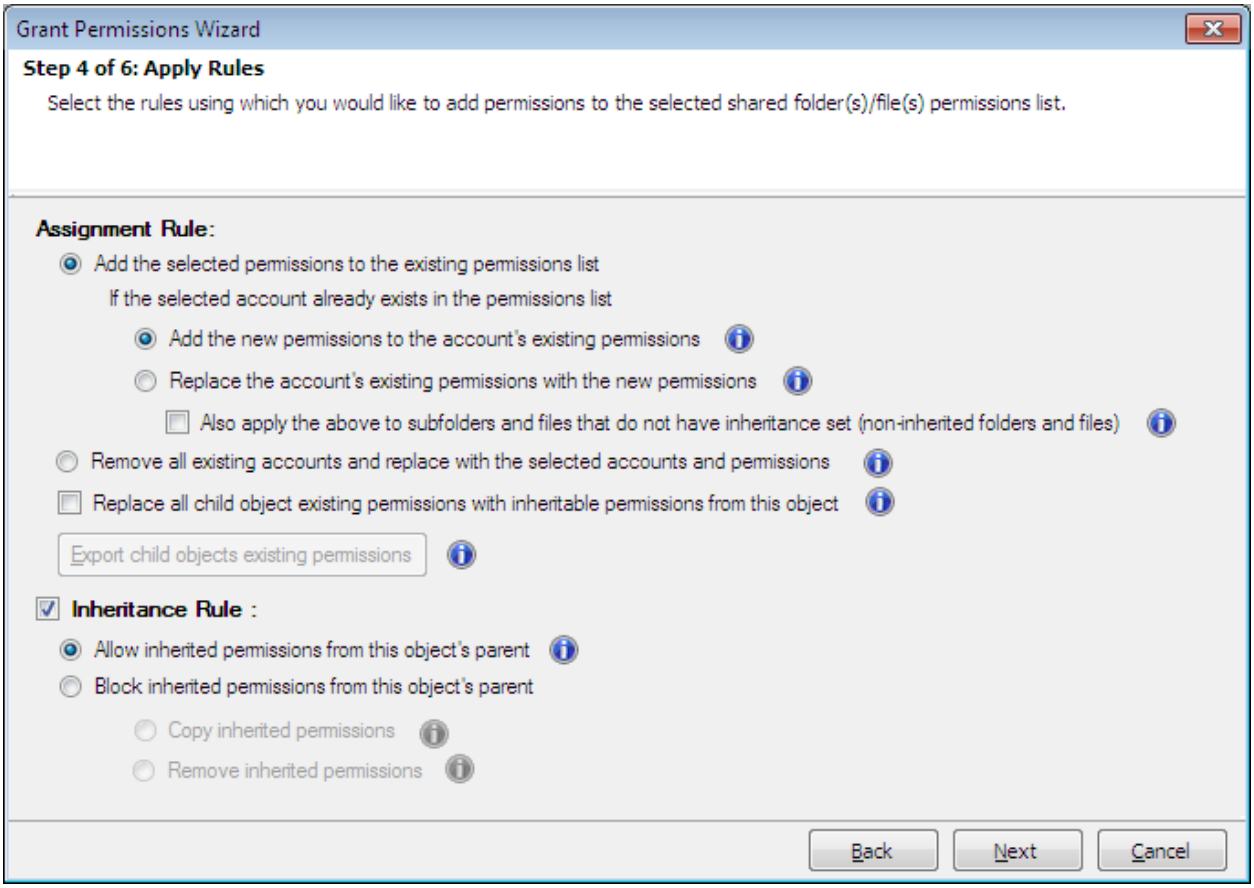
The Grant Permissions feature provides an option to Allow inheritable permissions from the parent object to the current shared folder(s)/file(s).

Click on 

button.

The Grant Permissions window will be displayed.

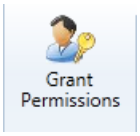
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?.
- In step 4 select the option Inheritance Rule and then select the option Allow inherited permissions from this object's Parent.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to block inherited permissions from the parent object to the current share?

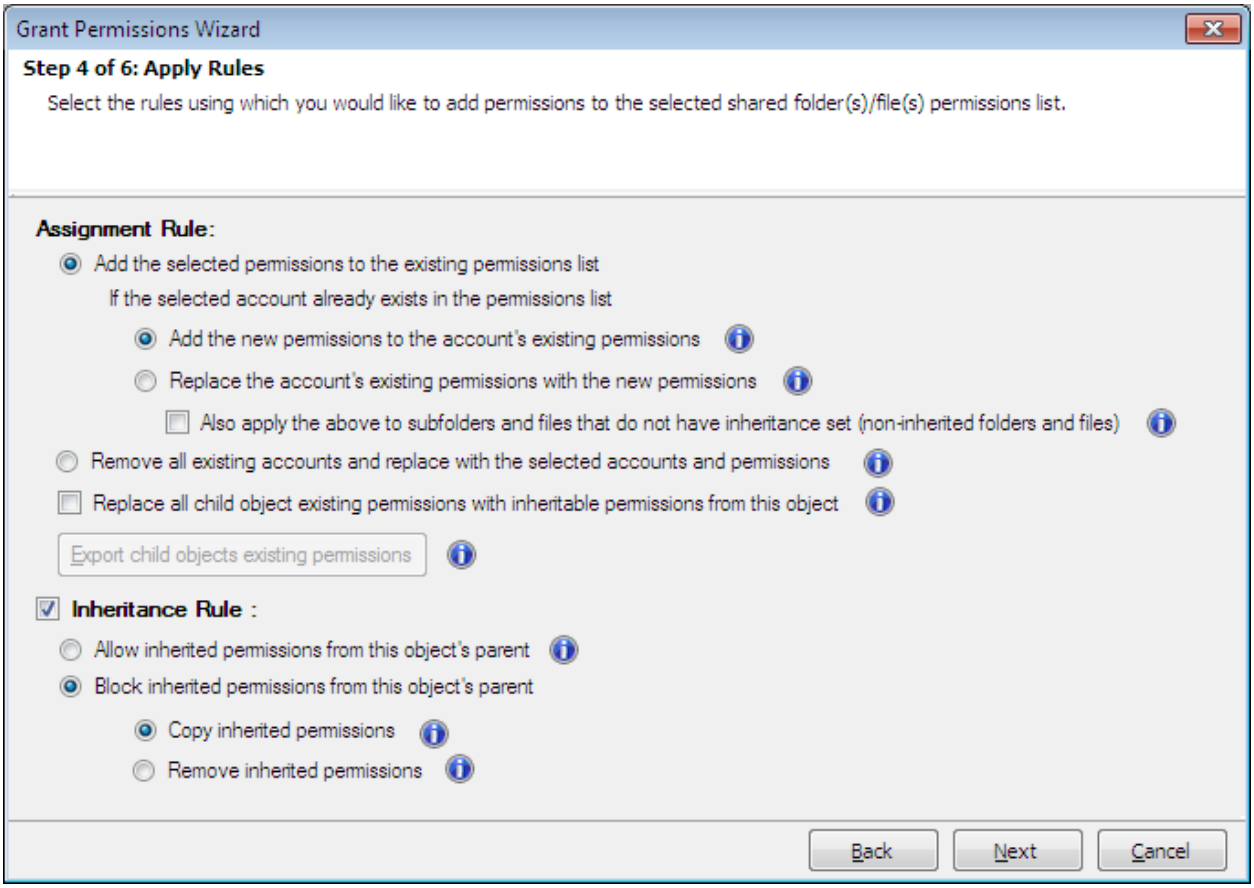
The Grant Permissions feature allows an option to Copy the inheritable permissions from the parent object to the current shares. This option will add the inherited permissions as explicit permissions in the Shares permissions list. You can also remove the inherited permissions from the parent object to the current shares.

Click on 

button.

The Grant Permissions window will be displayed.

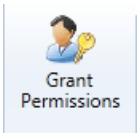
- Follow the steps 1 through 3 as outlined in How to Grant Permissions for selected Shares?
- In step 4 select the option Copy inherited permissions.
- If you wish to remove the inherited permissions, you may use the option Remove inherited permissions to remove all the inherited permissions from the parent object.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Grant Permissions for selected Shares?

How to Grant Permissions for selected Shares?

The **Grant Permissions** feature allows you to grant permissions to the Shares. You can use many options like Add the new permissions to the account's existing permissions, Replace the account's existing permissions with the new permissions, etc. You may select options to Allow, Block inheritance from the parent object and also Replace all child objects existing permissions with the inheritable permissions from this object while granting permissions for accounts.

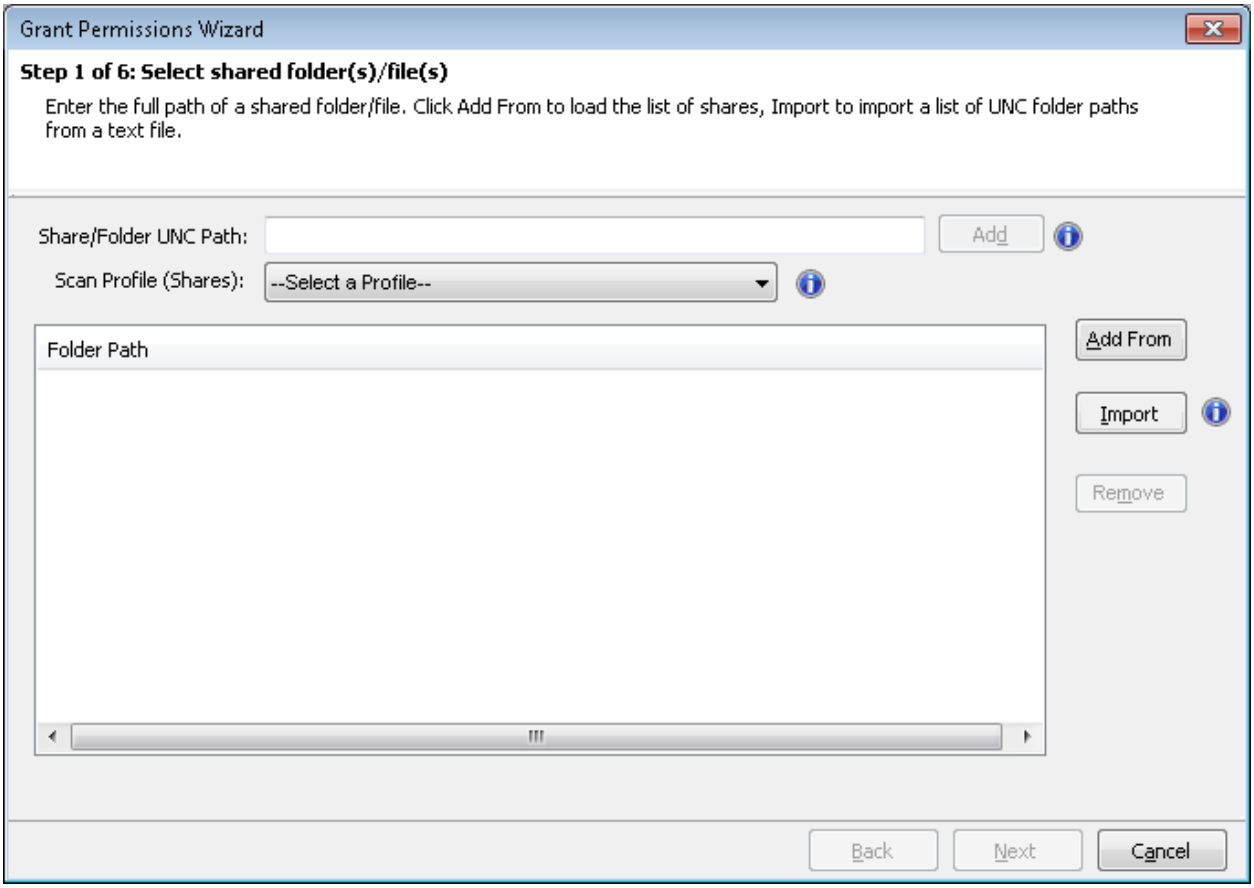
Click on 

button.

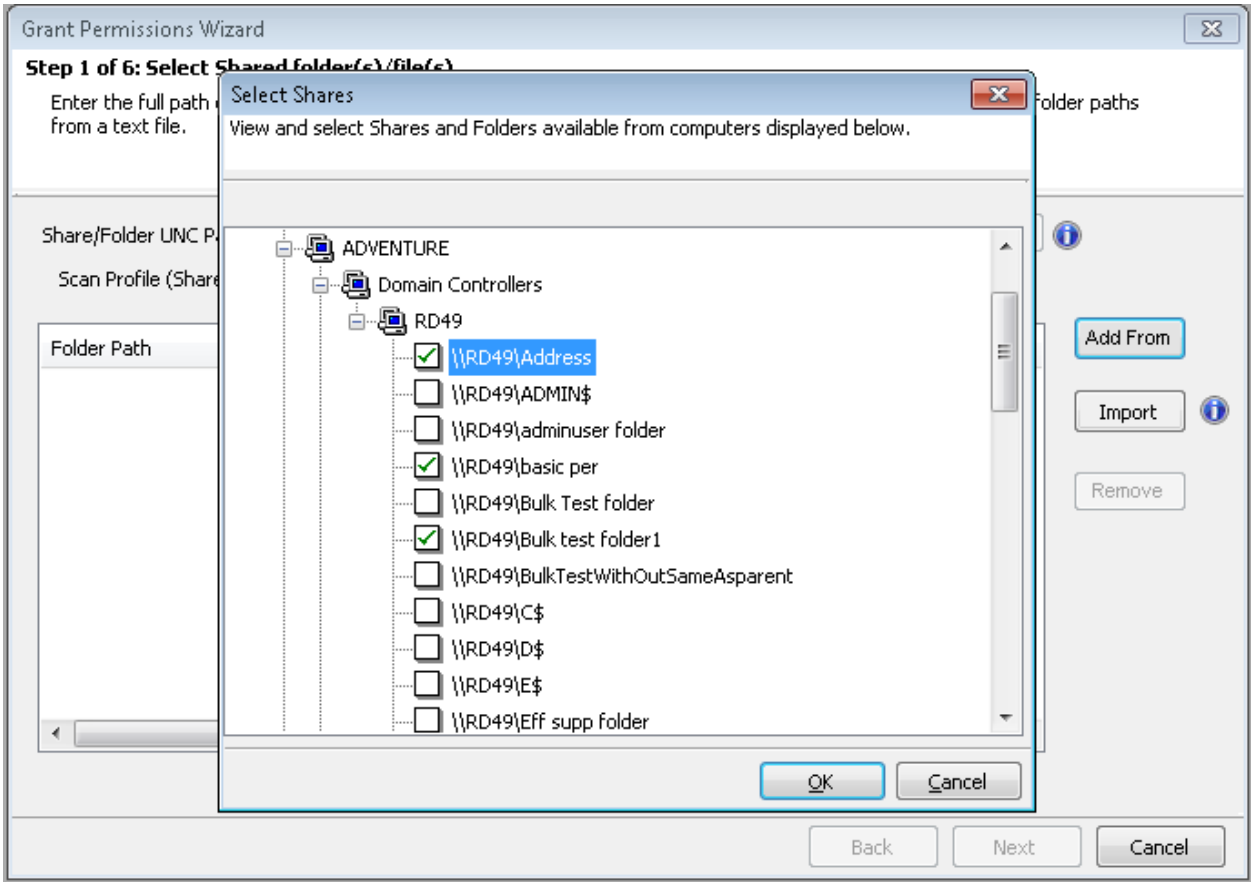
The Grant Permissions window will be displayed as shown below:

Step 1: Select shared folder(s)/file(s)

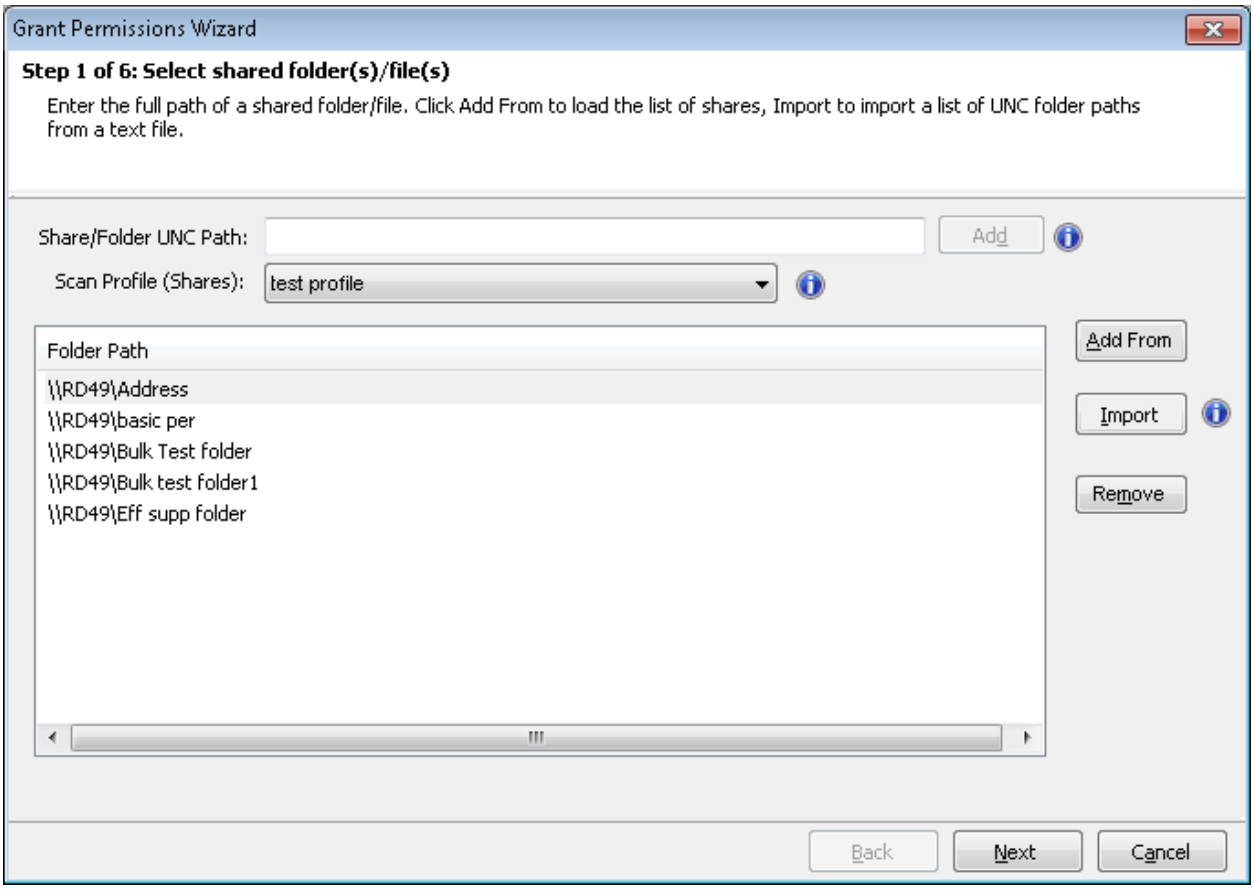
Select shared folder(s)/files by using any of the input options displayed


Grant Permissions Wizard
Step 1 of 6: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click **Add From** option
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use **Select a Scan Profile (Shares)** option to use the shares added in the profile.

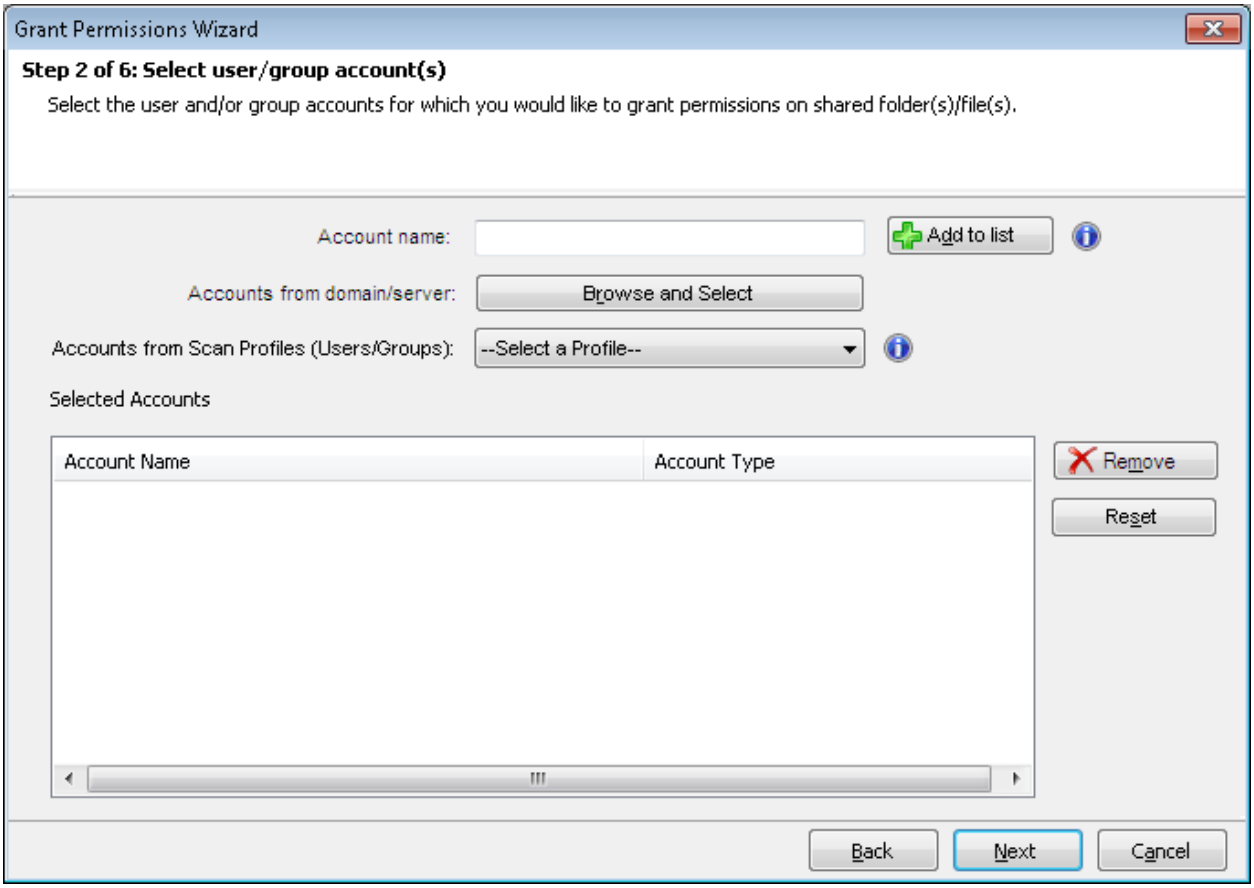


You may also type the UNC path of a shared folder that is not in the list and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared folder list from a text file by using the **Import** button.

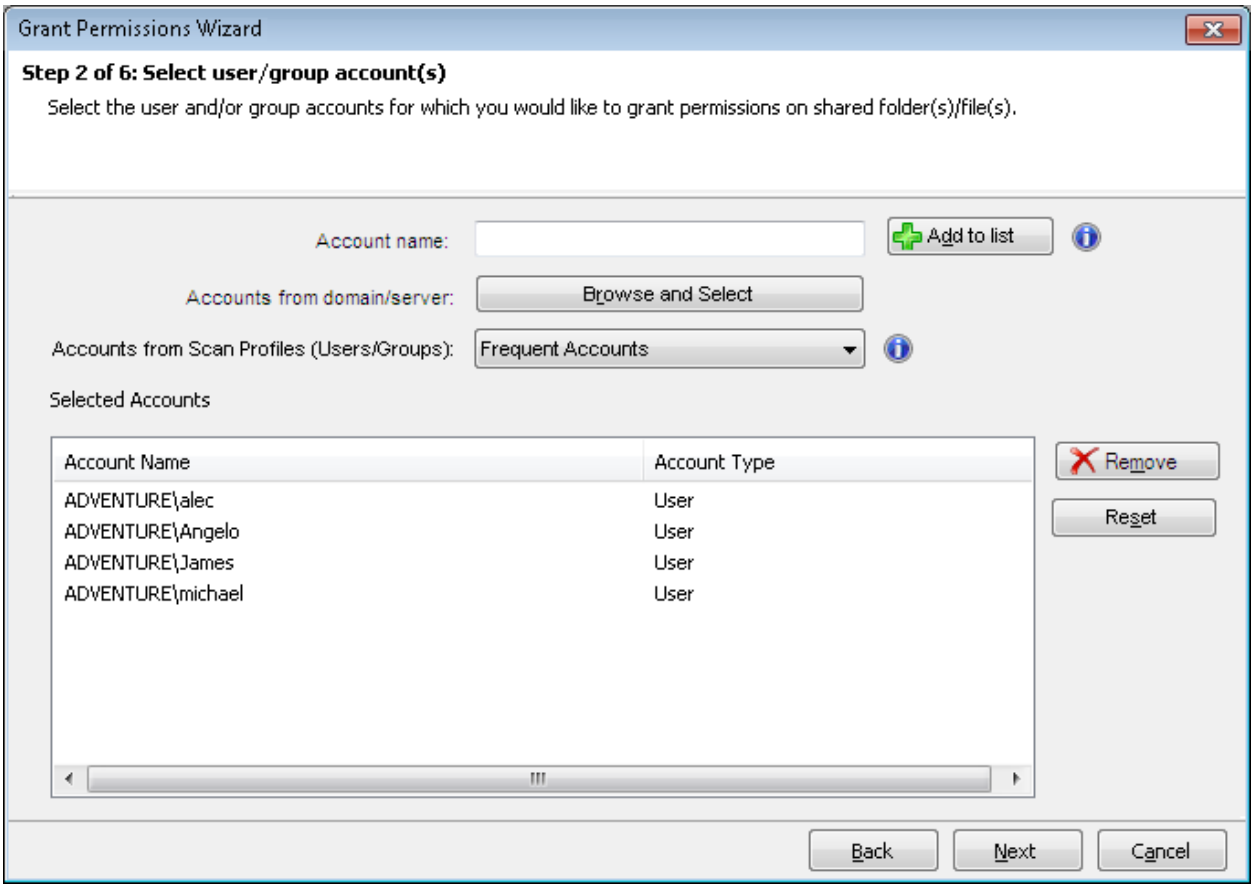
Click Next to proceed to the next step.

Step 2: Account Selection

1. Select the accounts, for which you wish to grant permissions.
2. The selected accounts will be added to the wizard as shown below:



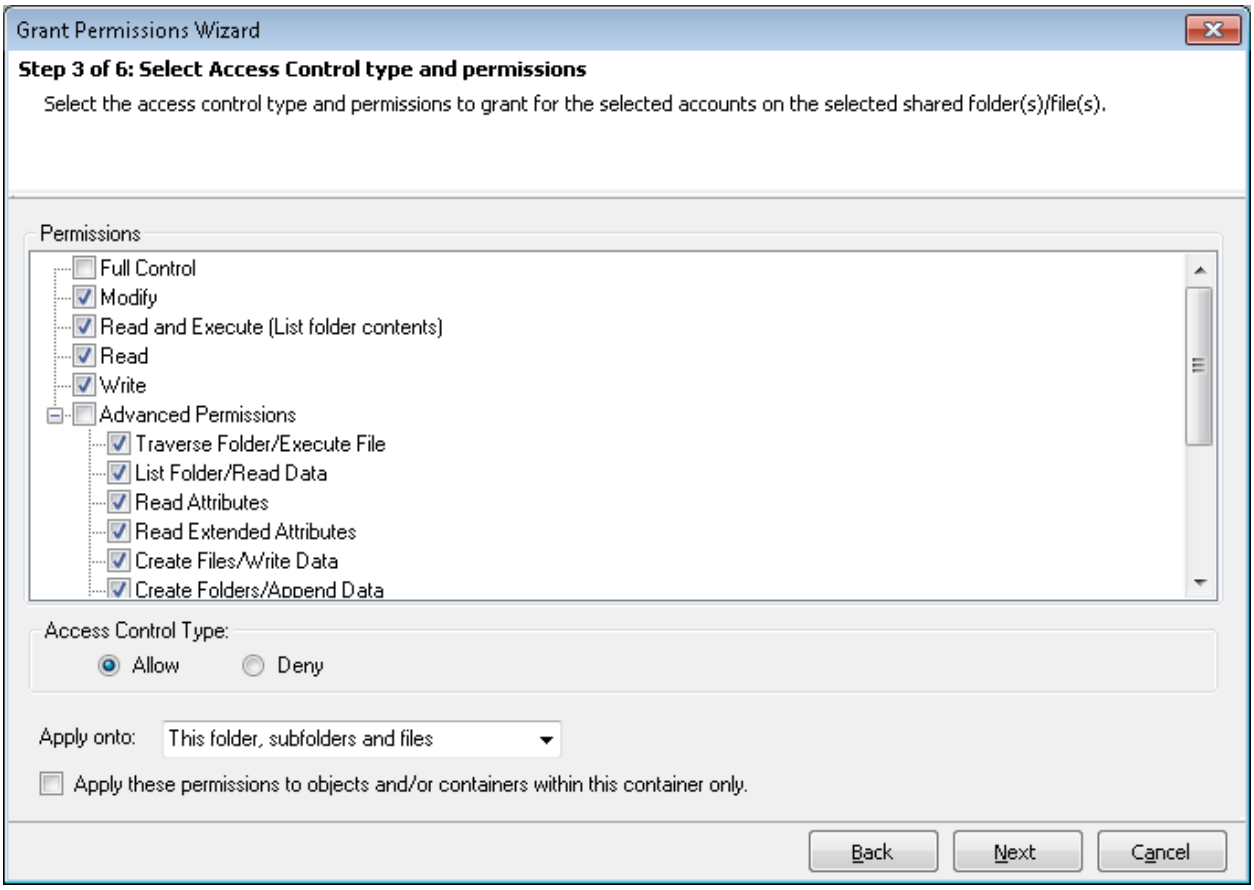
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile.



Click **Next** to proceed to the Next step.

Step 3: Select Access Control type and permissions

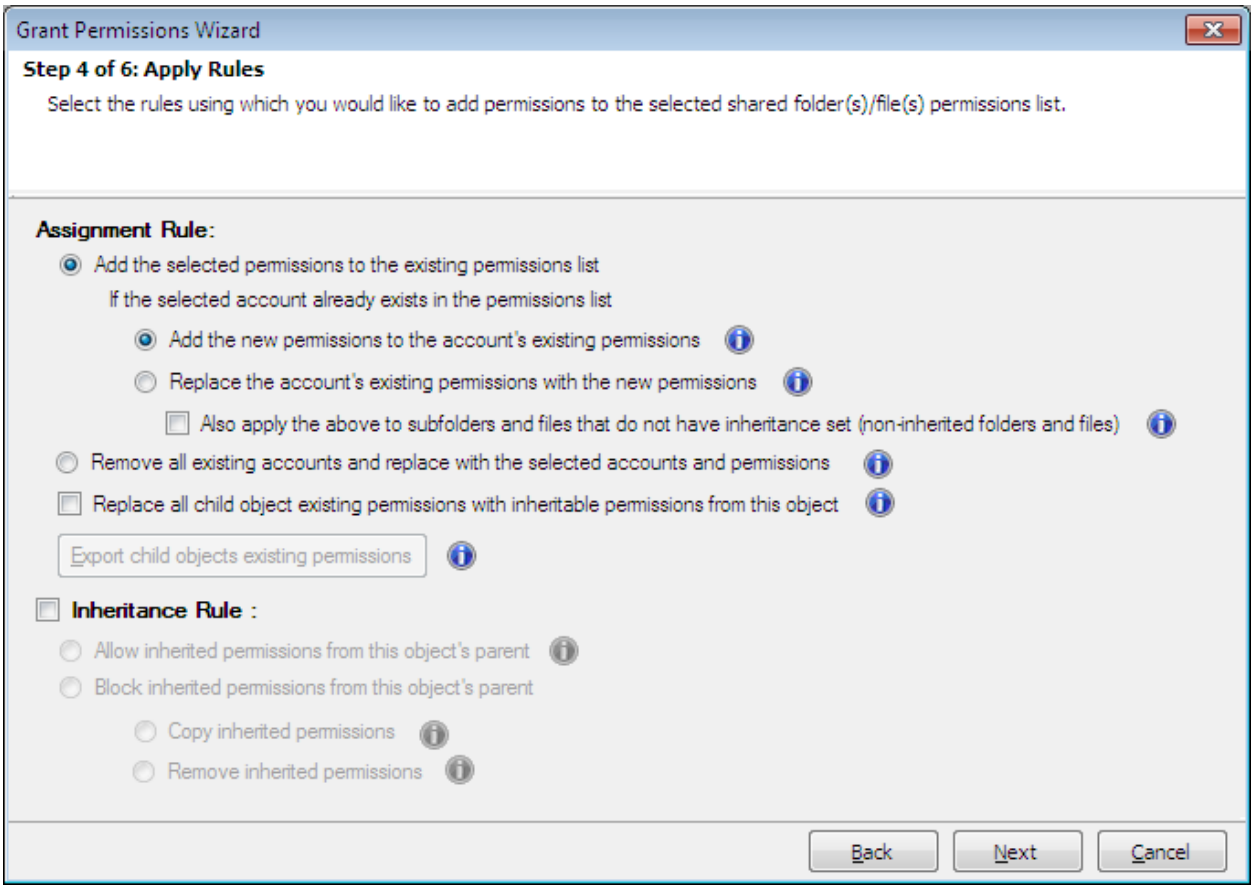
Select ACE type and permissions to grant for the selected accounts on the selected shared folder(s) /files(s)



Click **Next** to proceed to the next step.

Step 4: Apply the required rules to be used while assigning permissions

Select which rules to apply while assigning permissions.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

Add the new permissions to the account's existing permissions option will add the selected permissions to the existing permissions list and also it will not affect the existing permissions.

You may also use the below options to grant permissions and also apply inheritance by Inheritance rule

- Replace the account's existing permissions with the new permissions.
- Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files).
- Remove all existing accounts and replace with the selected accounts and permissions.
- Replace all child objects existing permissions with the inheritable permissions from this object.

Inheritance Rule:

- Allow inherited permissions from this object's parent.
- Copy inherited permissions.
- Remove inherited permissions.

Replace the account's existing permissions with the new permissions

If a selected account already exists in the current list of permissions of the selected shared folder(s)/file(s), this option will replace all explicitly assigned account permissions with the newly selected permissions for that account.

Example: If the share already has some accounts with permissions like Allow Read and Write and if the same existing accounts selected with permissions Deny Modify to grant permissions then this option will replace the existing accounts previous permissions (Allow Read and Write) with new permission (Deny Modify). Otherwise if the selected account not exist in the share permissions list then it will add into the permissions list.

Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)

This option will grant permissions to the selected accounts on subfolders and files that do not have inherited permissions from its parent object with respect to the above options.

Note: If this option is checked, the subfolders and files must have the applicable rights for the owner or the currently logged on user to perform this operation.

Example: If the share has some subfolders and files with the blocked inheritance then this option will assign permissions based on the selected options.

Remove all existing accounts and replace with the selected accounts and permissions

This option will remove all existing accounts that have explicitly assigned permissions for the selected shared folder(s)/file(s) and replace them with the selected accounts and permissions. Note that this will not remove inherited permissions from parent folder.

Caution: All existing account permissions will be cleaned up completely and the newly selected permissions will be applied.

Example: If the share has 7 accounts then this option will remove all the 7 accounts and replace with the new selected accounts and permissions.

Replace all child objects existing permissions with the inheritable permissions from this object

This option will remove explicitly defined permissions on all descendants of the selected shared folder(s)/file(s) and replace them with inheritable permissions from the selected shared folder(s)/file(s).

Example: If the share has some subfolders with the explicitly assigned permissions and some subfolders with blocked inheritance then this option will remove all explicitly assigned permissions of subfolders and allow inherited permissions from the parent object.

Allow inherited permissions from this object's Parent

This option will allow the selected shared folder(s)/file(s) to inherit permissions from its parent object.

Example: If the share do not have any inherited permissions and the inheritance from the parent object blocked then this option will allow inherited permissions from the parent object.

Copy inherited permissions

This option will copy the permission entries that were previously inherited from the parent to this selected shared folder(s)/file(s).

Example: If the share already allowed to inherit permissions from parent object then this option will remove the inheritance and add the inherited permissions as explicit permissions in the permissions list.

Remove inherited permissions

This option will remove the permission entries that were previously inherited from the parent and keep only those permissions explicitly defined/granted here.

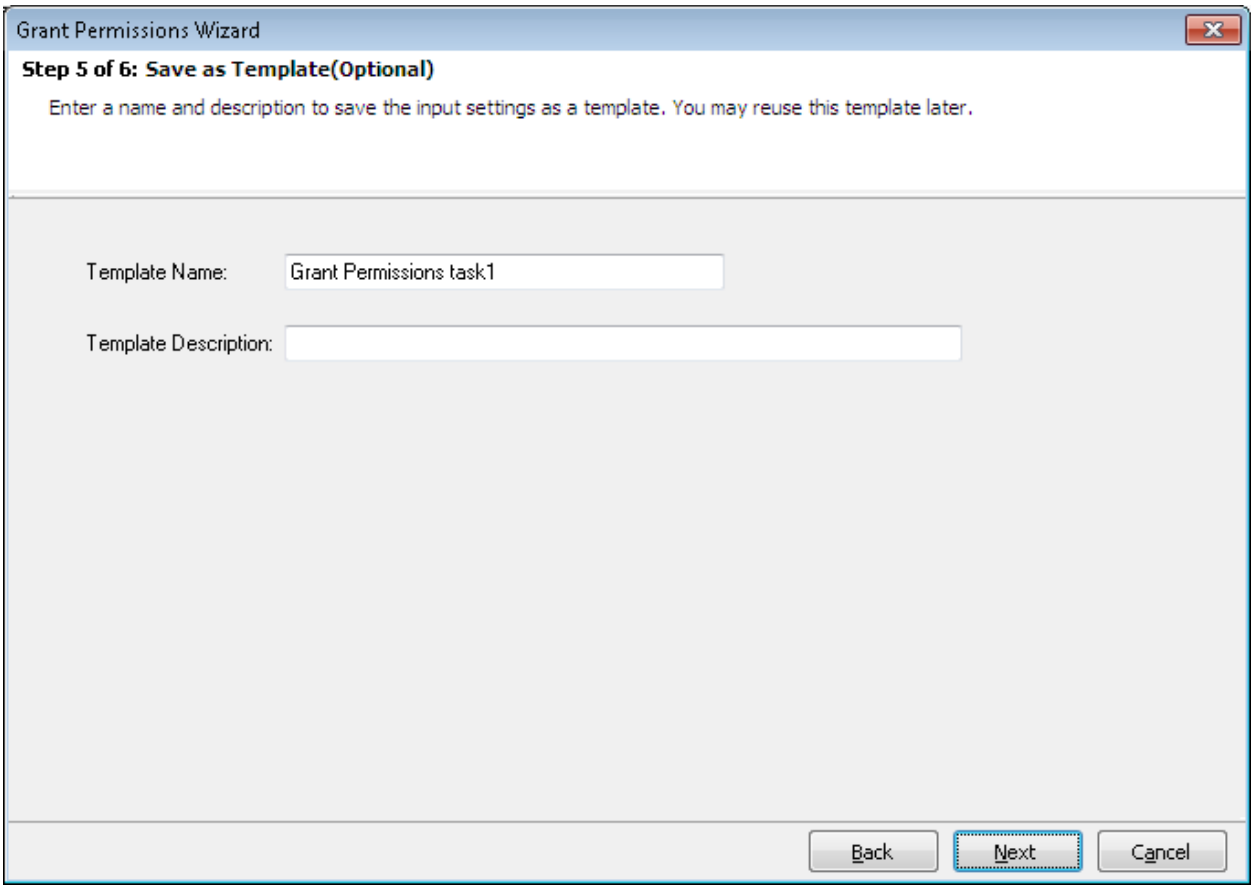
Caution: Removing permission inheritance from parent may break permissions/policies designed with the default inheritance option enabled. Use this option after a careful review.

Example: If the share is already set to inherit permissions from parent object then this option will remove the inheritance from parent object.

Click Next to proceed to the Next step

Step 5: Save as template

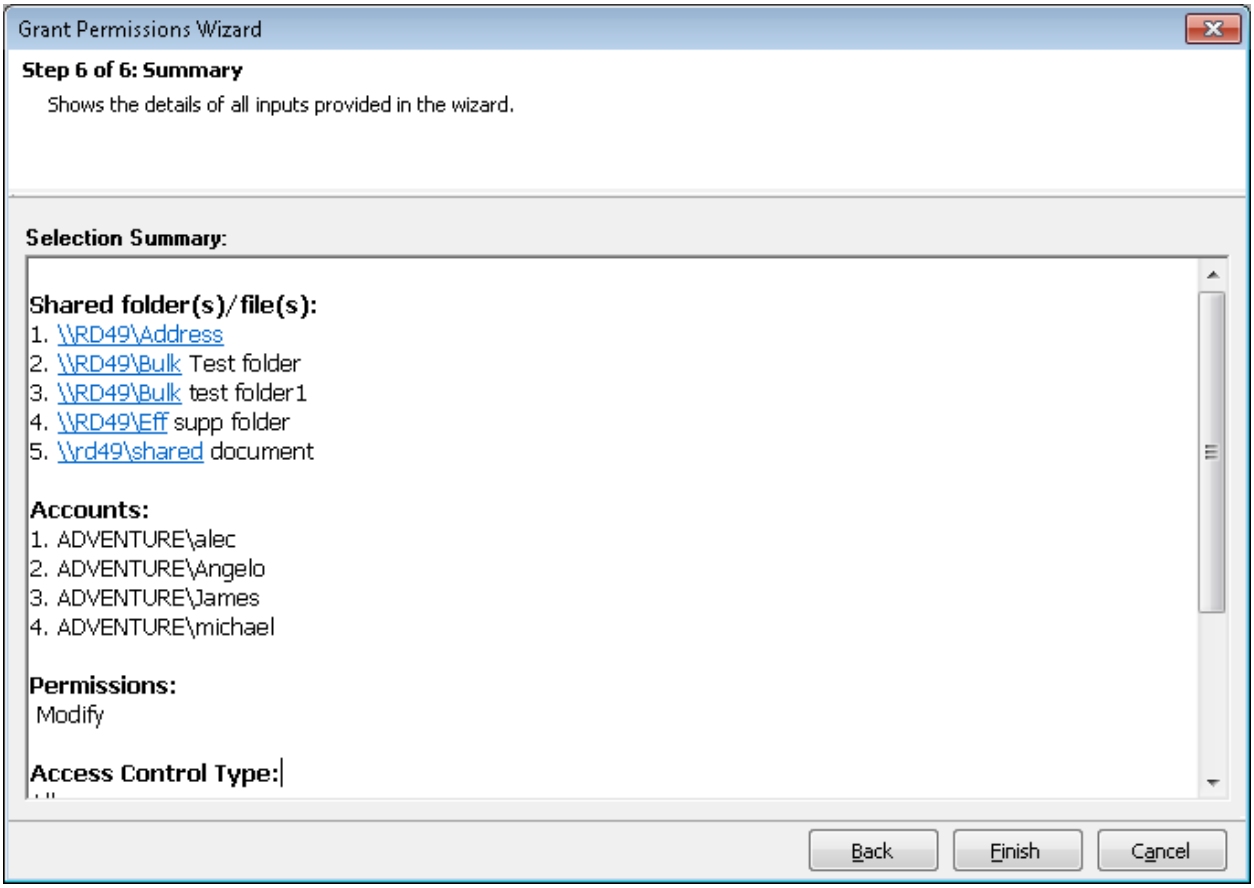
Enter a name and description to save these settings as a template for reuse later.


Grant Permissions Wizard
Step 5 of 6: Save as Template(Optional)
Enter a name and description to save the input settings as a template. You may reuse this template later.
Template Name:
Grant Permissions task1
Template Description:
Back
Next
Cancel

Click **Next** to proceed to the next step

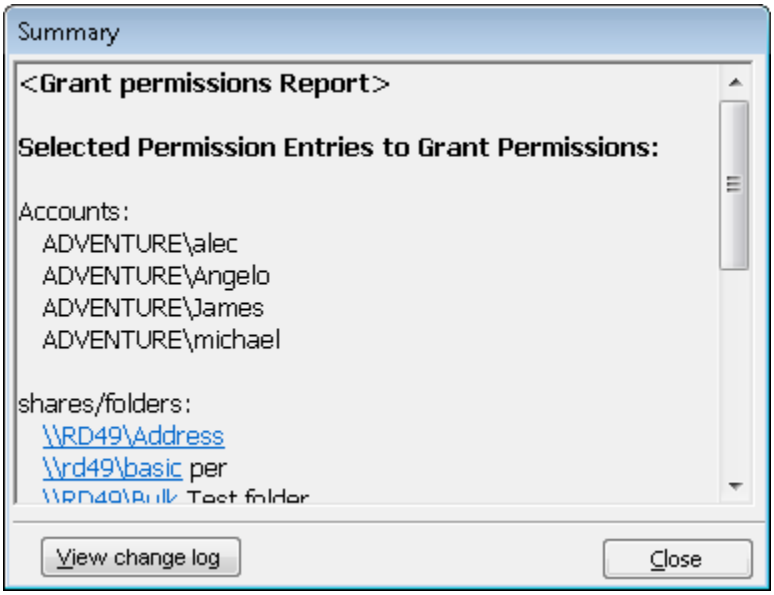
Step 6: Summary

This step displays the summary of all the input data along with the selected options.



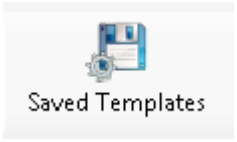
Click **Finish** to complete the Grant Permissions wizard.

Permissions will be granted as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.

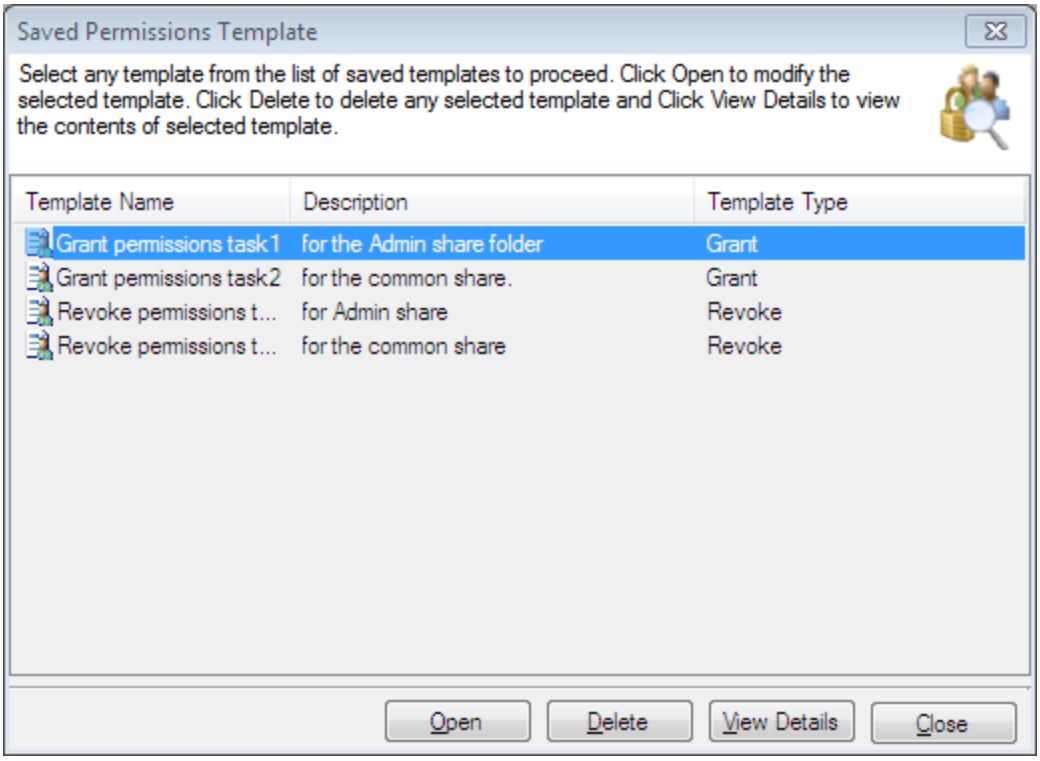

Summary
<Grant permissions Report>
Selected Permission Entries to Grant Permissions:
Accounts:
ADVENTURE\alec
ADVENTURE\Angelo
ADVENTURE\James
ADVENTURE\michael
shares/folders:
\\RD49\Address
\\rd49\basic per
View change log
Close

How to reuse the Grant Permissions template?

The Saved Templates contains the list of saved templates to Grant and Revoke Permissions.

Click on 

button. The Saved Templates window will be displayed as shown below.



The saved templates window allows you to perform the following operations:

- Open an existing template
- Delete a template
- Preview the contents of a template

Open an existing Template

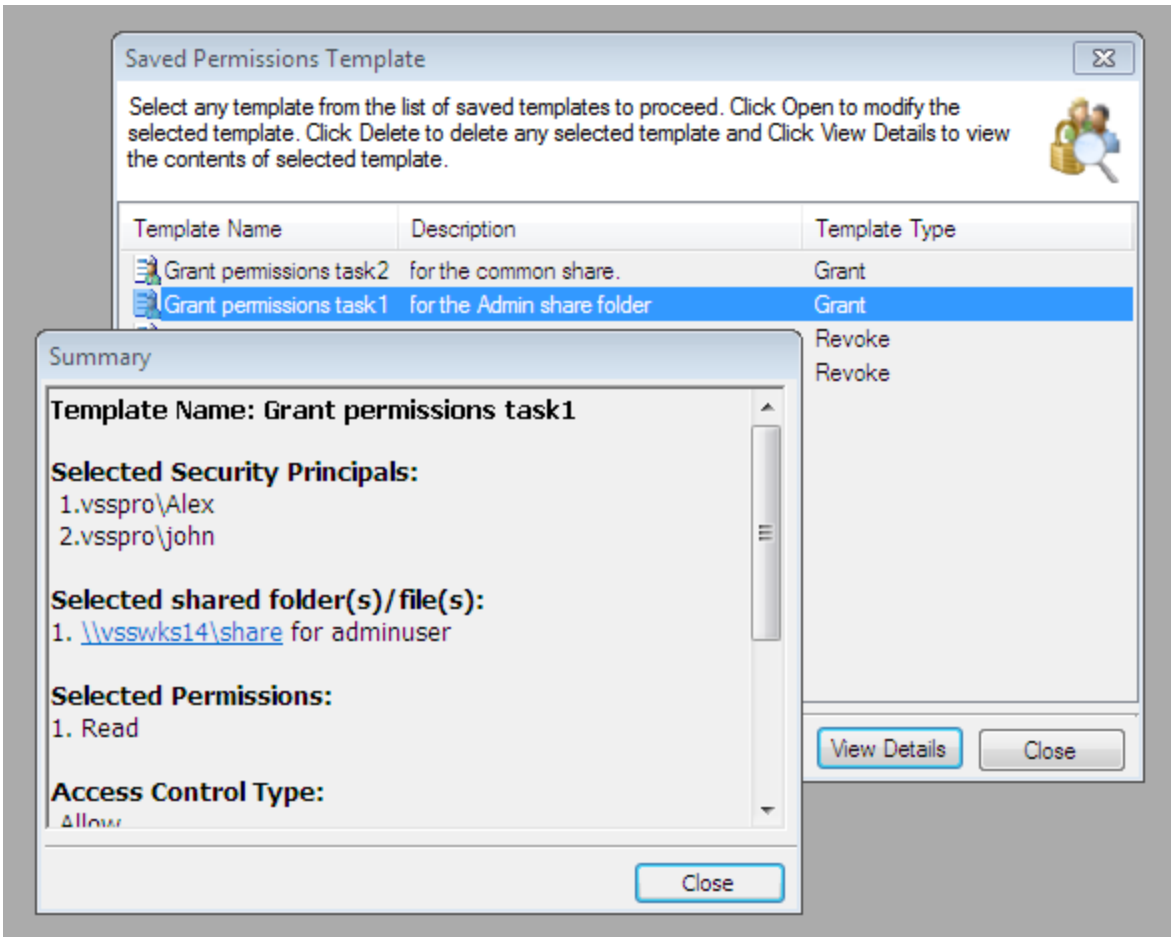
1. To open an existing Grant permissions template, select the Grant permissions template and click Open button in the window. The Grant permissions Dialog will appear on the screen which will allow you to edit the selected template.
2. During edit operation you can modify the computer list and permissions entries, however, you cannot modify the name of the template.

Delete a template

To delete a Grant permissions template, select a Grant permissions template which you want to delete, and then click **Delete** button. The selected template will be deleted permanently.

Preview the settings of a Template

To preview the settings of a saved Template, select a saved Grant permissions template, and then click **View Details** button. The settings will be displayed in a window as shown below:



Revoke Permissions

About Revoke Permissions

How to revoke permissions from the selected shares permissions list?

How to reuse the revoke permissions template?

About Revoke Permissions

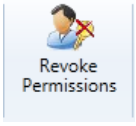
The Revoke Permissions feature provides many options to remove Accounts and their permissions from the existing list of ACE entries in shared Folders and Files. You may revoke all existing explicit Accounts and also you may selectively revoke a set of permissions granted to accounts. Here is the list of actions you can perform using the Revoke Permissions feature.

Note: This feature will not break the inheritance from the parent of current object. If you still wish to break the inheritance from the parent object, you may use the Grant Permissions or Modify Permissions feature to block inheritance.

Actions
Revoke permissions from the selected shares permissions list: (How to?)
Remove the selected Account with the selected permissions from the shared folder(s)/file(s) permissions list.
Revoke the selected permissions from all existing explicit accounts in shares permissions list: (How to?)
Revoke the selected permissions from all existing explicit Accounts in the share permissions list.
Revoke the exact matching permissions from the existing explicit accounts in the shares permissions list: (How to?)
Revoke existing explicit accounts, only if the selected permissions match exactly with the ACE entries in the shares permissions list.
Revoke all existing explicit permissions from the shares permissions list: (How to?)
Revoke the selected permissions from all existing explicit accounts in the share permissions list.
Revoke the exact matching permissions from the shares permissions list: (How to?)
Revoke the selected accounts, only if the selected permissions match exactly with the ACE entries in the shares permissions list.
Revoke the selected Accounts and all their permissions from the shares permissions list: (How to?)
Revoke the selected Accounts with all existing explicit permissions in the shares permissions list.
Revoke the Orphaned SIDs from the selected shares permissions list: (How to?)
Remove the Orphaned SIDs from the shared folder(s)/file(s) permissions list.

How to revoke the selected permissions from all existing explicit accounts in the share permissions list?

The Revoke Permissions feature allows an option to revoke selected permissions from all existing explicit accounts in the share permissions list.

Click on 

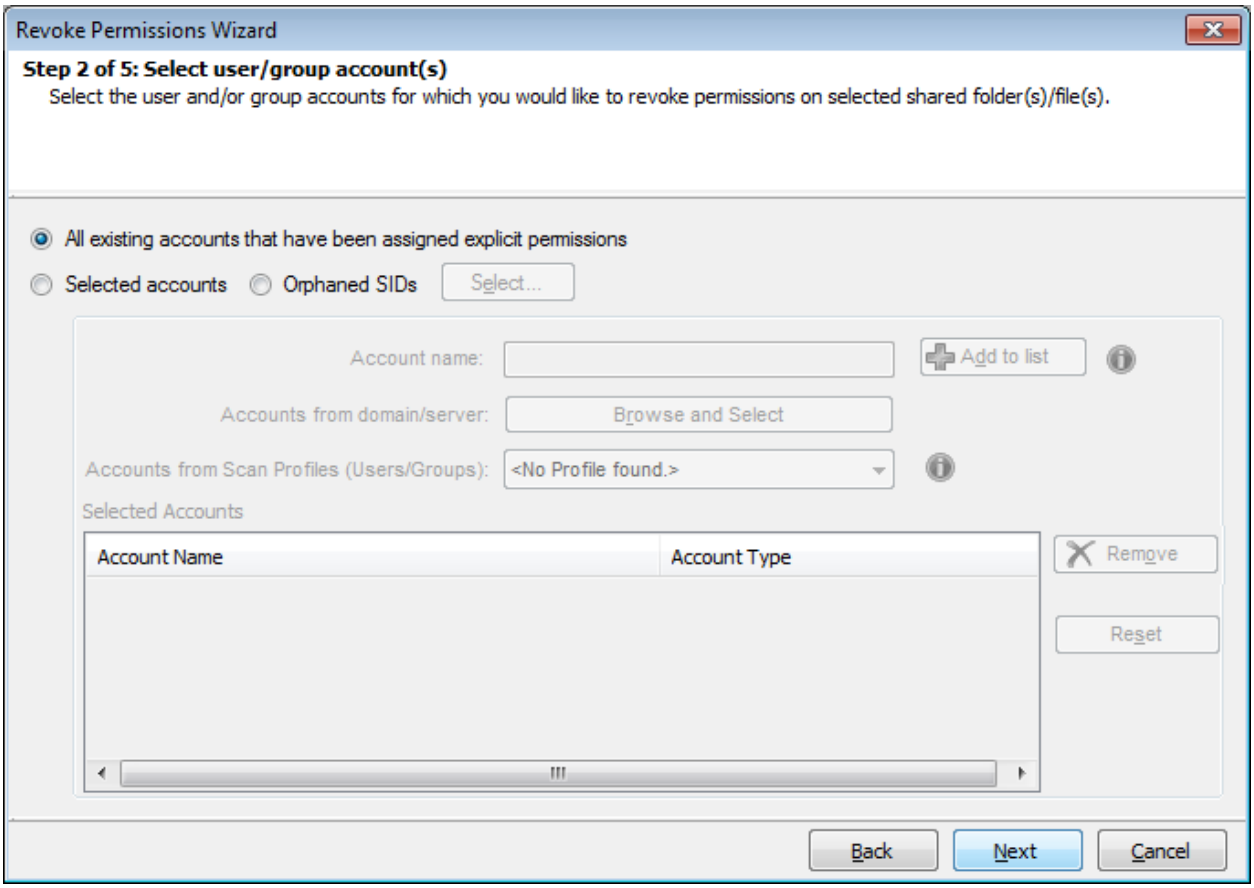
button.

The Revoke Permissions window will be displayed.

- Follow the steps 1 through 2 as outlined in How to Revoke permissions from the selected shares permissions list?

Step 3: User and/or Group selection

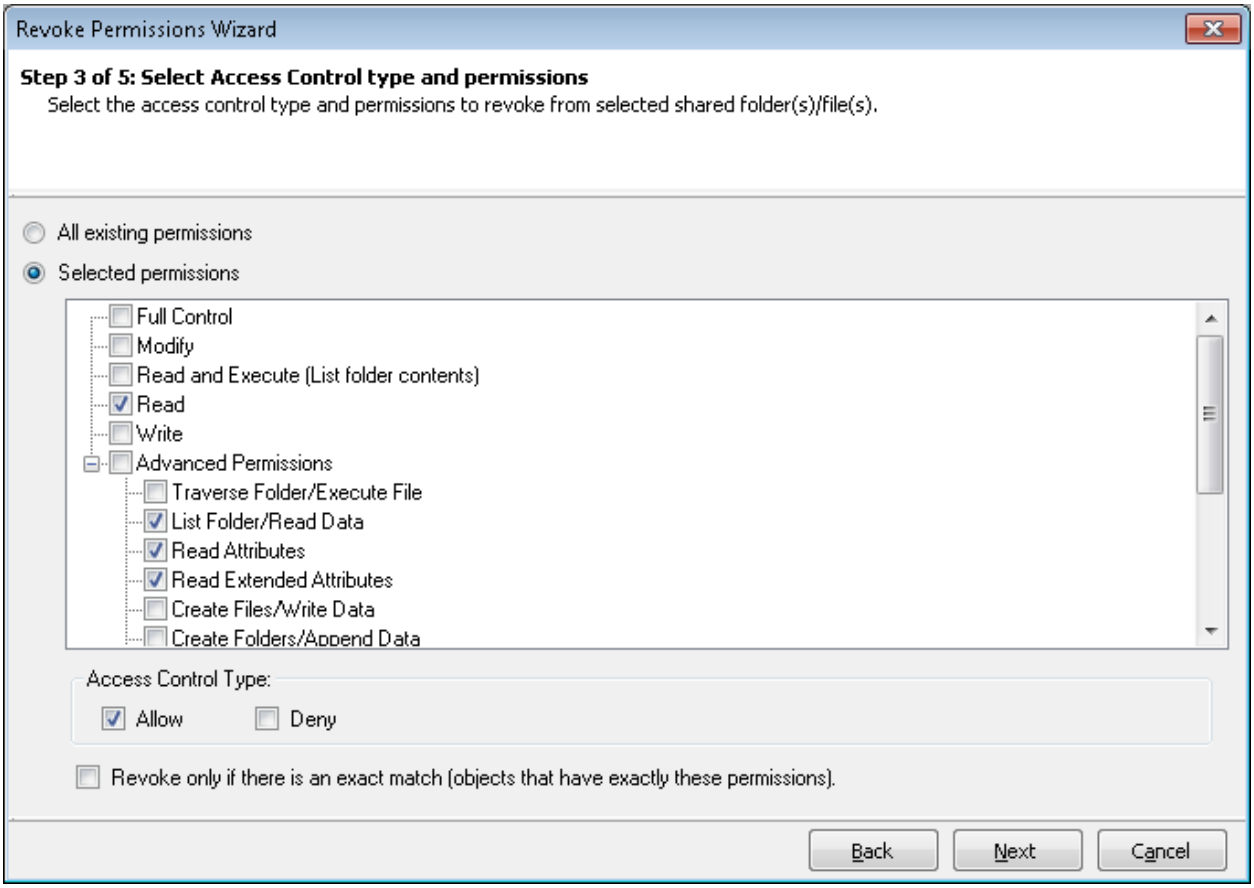
Select the option **All existing accounts that have been assigned explicit permission**.



Click **Next** to proceed to the next step.

Step 4: Select Access Control type and permissions

Click the option **Selected permissions** and select the ACE type and permissions

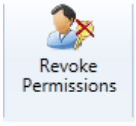


Click **Next** to proceed to the next step.

Follow the steps 5 through 6 as outlined in [How to Revoke Permissions from selected Shares permissions list?]

How to revoke the exact matching permissions from the existing explicit accounts in the share permissions list?

The **Revoke Permissions** feature allows an option to revoke existing explicit accounts, only if the selected permissions match exactly with the ACE entries in the shares permissions list.

Click on 

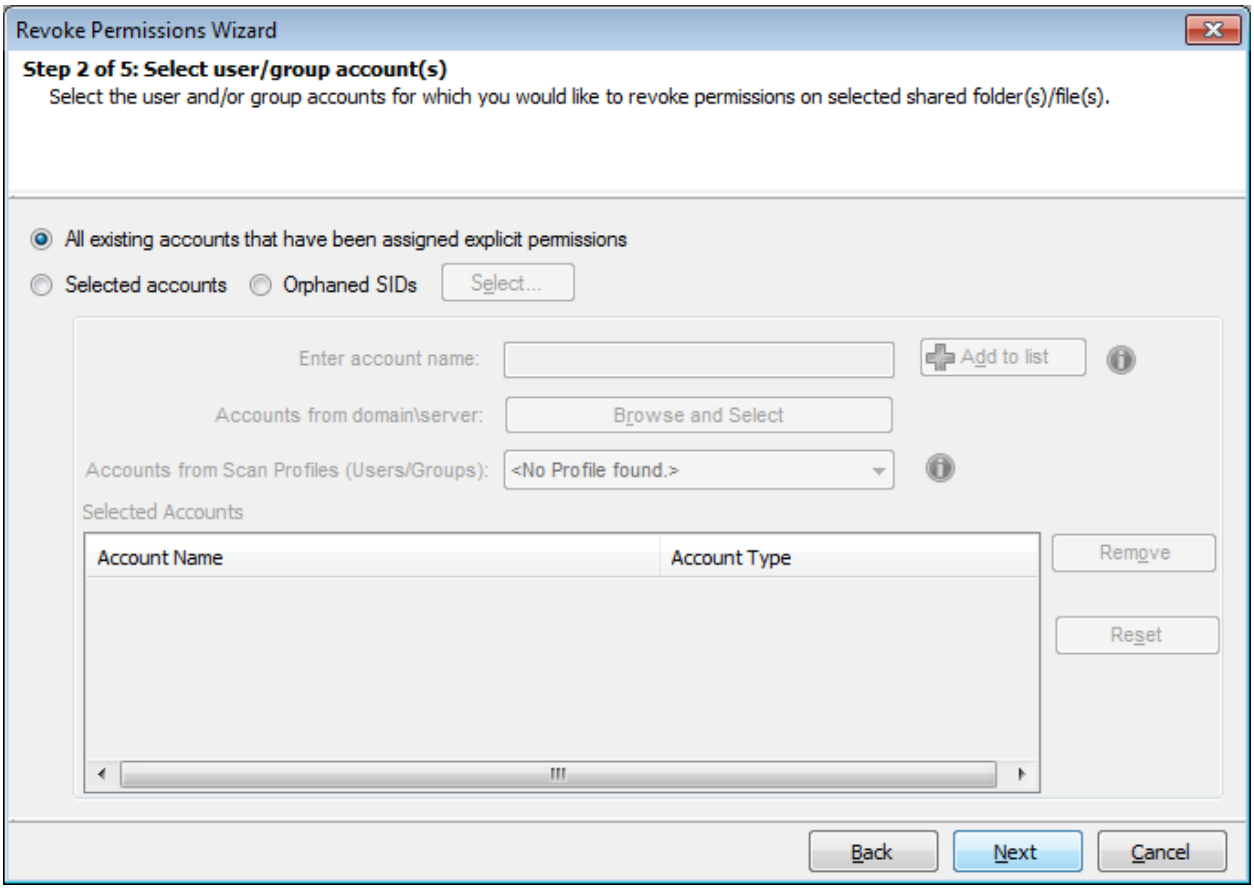
button.

The Revoke Permissions window will be displayed.

- Follow the steps 1 through 2 as outlined in How to Revoke Permissions from selected Shares permissions list?

Step 3: Account selection

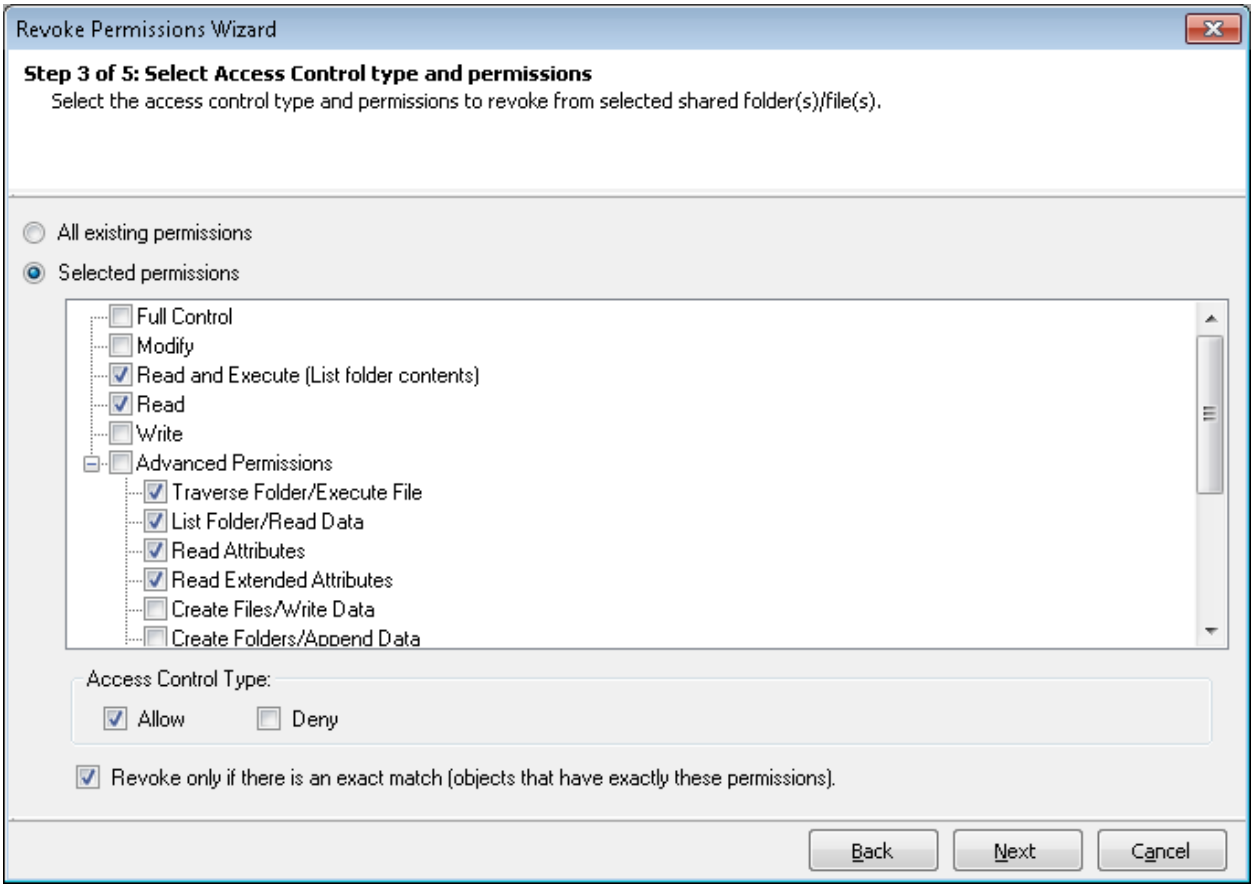
Select the option **All existing accounts that have been assigned explicit permissions**.



Click **Next** to proceed to the next step.

Step 4: Select Access Control type and permissions

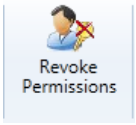
Select ACE type, permissions and also select the option **Revoke only if there is an exact match**



- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in [How to Revoke Permissions from selected Shares permissions list?]

How to revoke all existing explicit permissions from the shares permissions list?

The **Revoke Permissions** feature allows an option to revoke all existing explicit accounts in the shares permissions list.

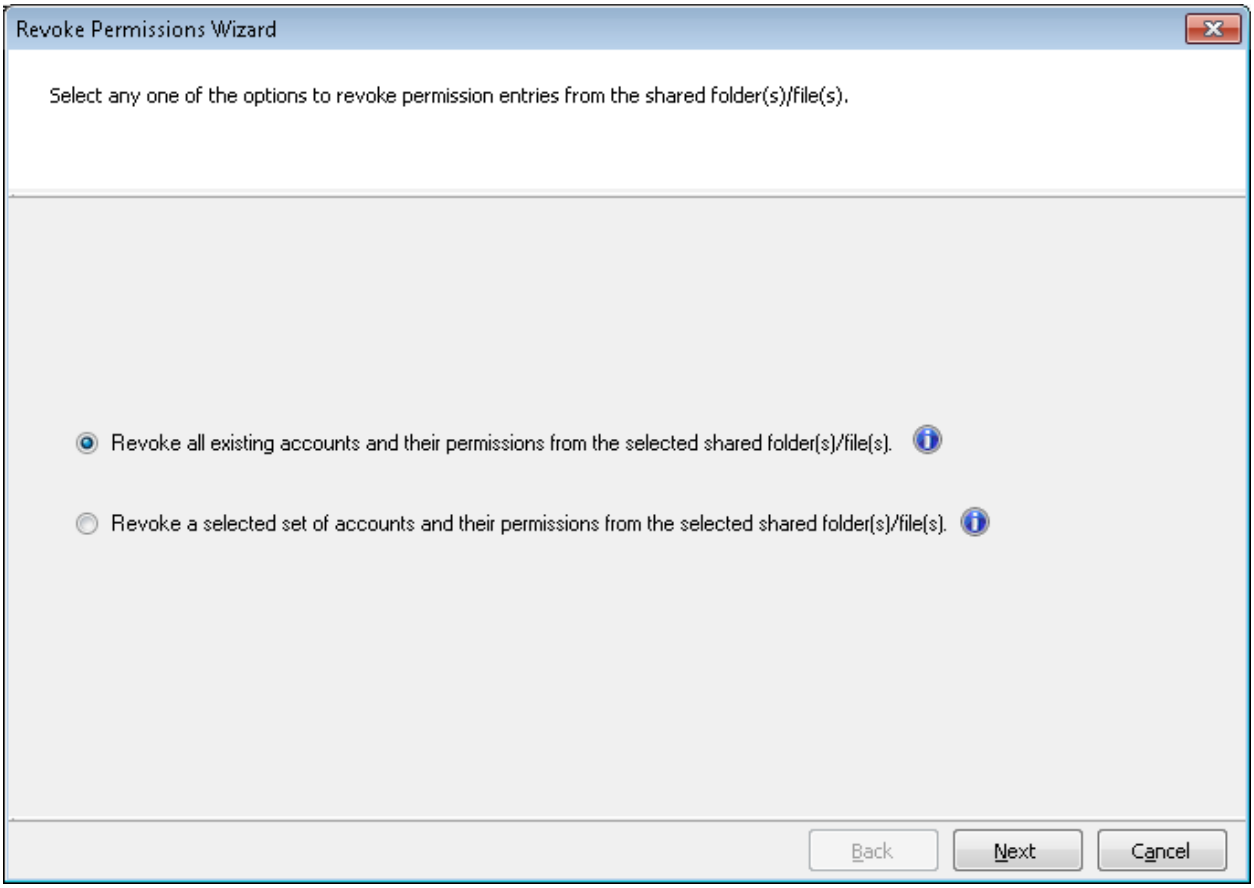
Click on 

button.

The Revoke Permissions window will be displayed as shown below:

Step 1: Select a Revoke permissions option

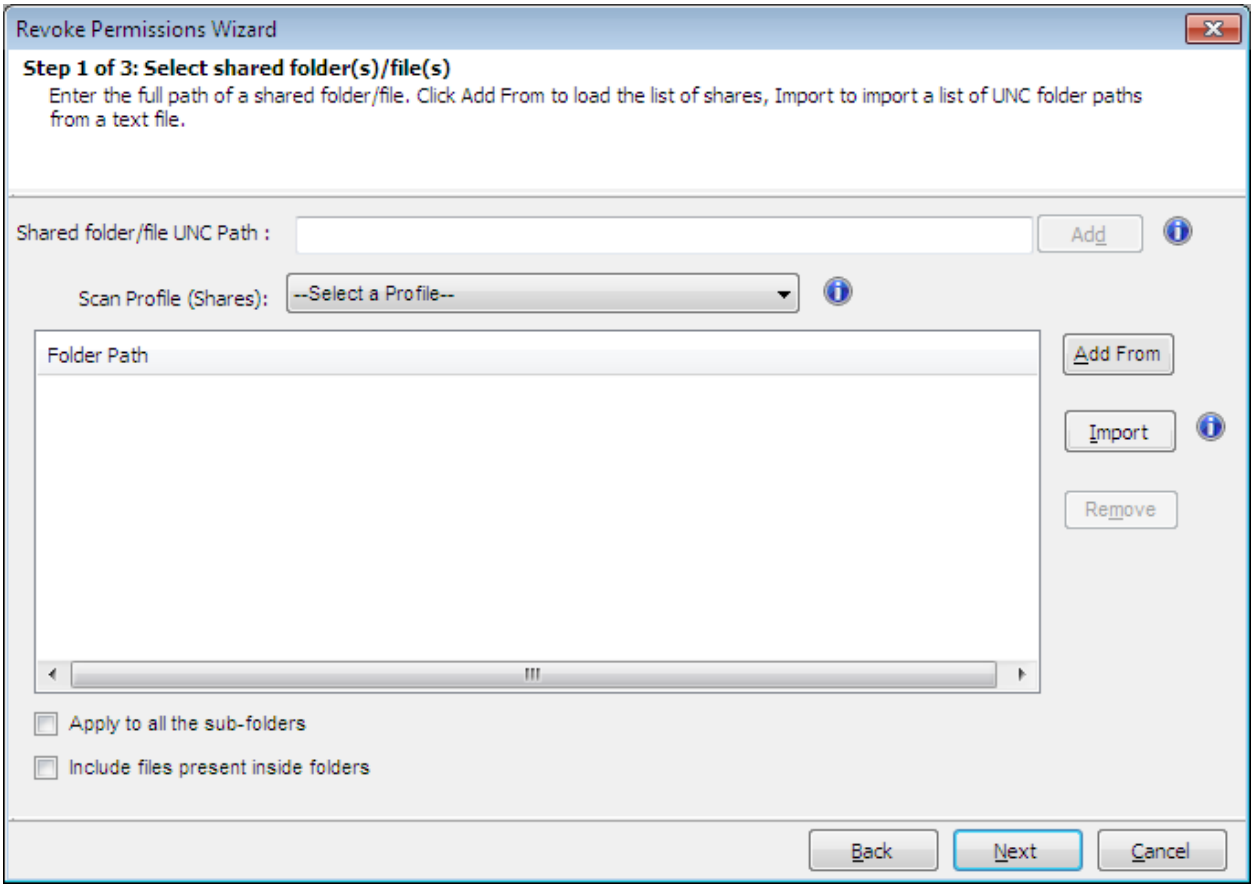
Select the option **Revoke all existing accounts and their permissions from the selected shared folder(s)/file(s)**


Revoke Permissions Wizard
Select any one of the options to revoke permission entries from the shared folder(s)/file(s).
Revoke all existing accounts and their permissions from the selected shared folder(s)/file(s).
Revoke a selected set of accounts and their permissions from the selected shared folder(s)/file(s).
Back
Next
Cancel

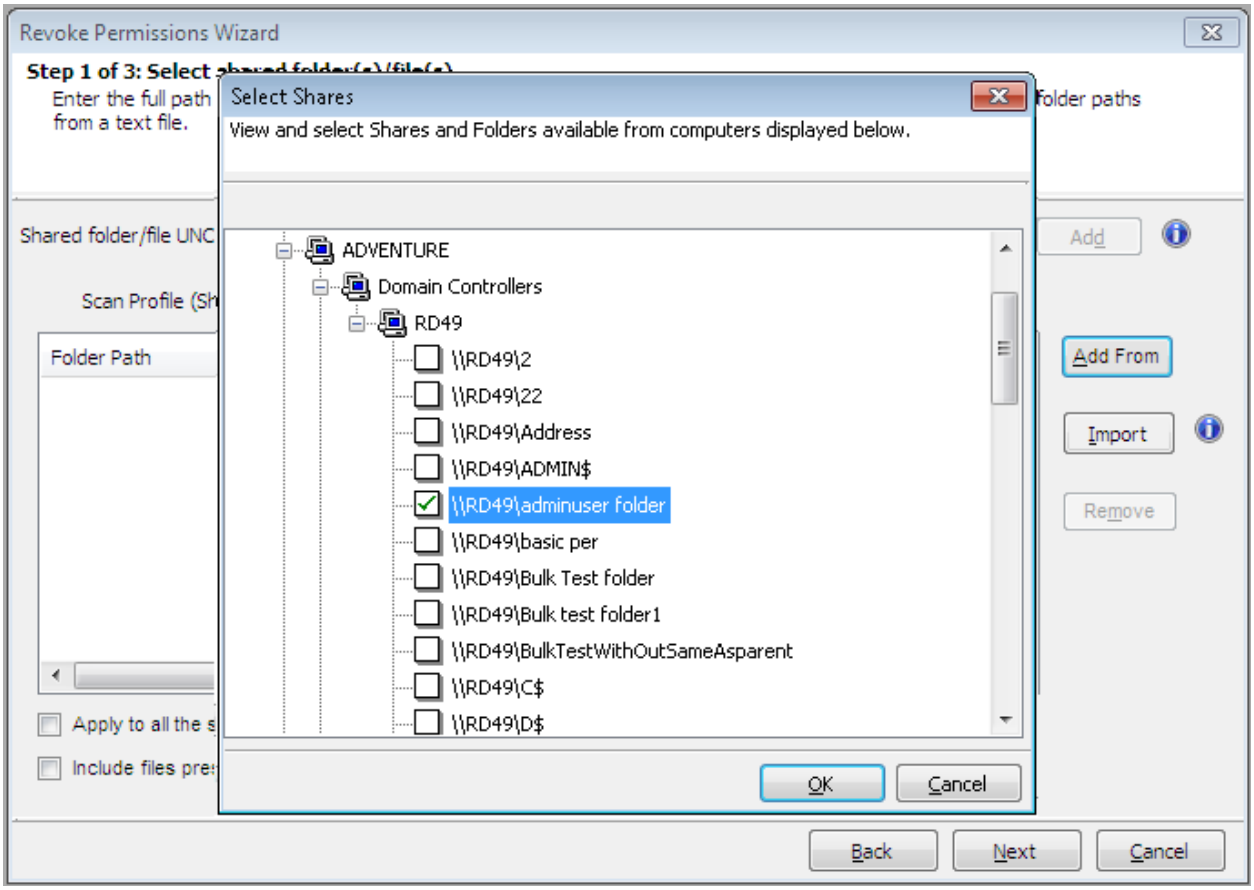
Click **Next** to proceed to the Next step.

Step 2: Select shared folder(s)/file(s)

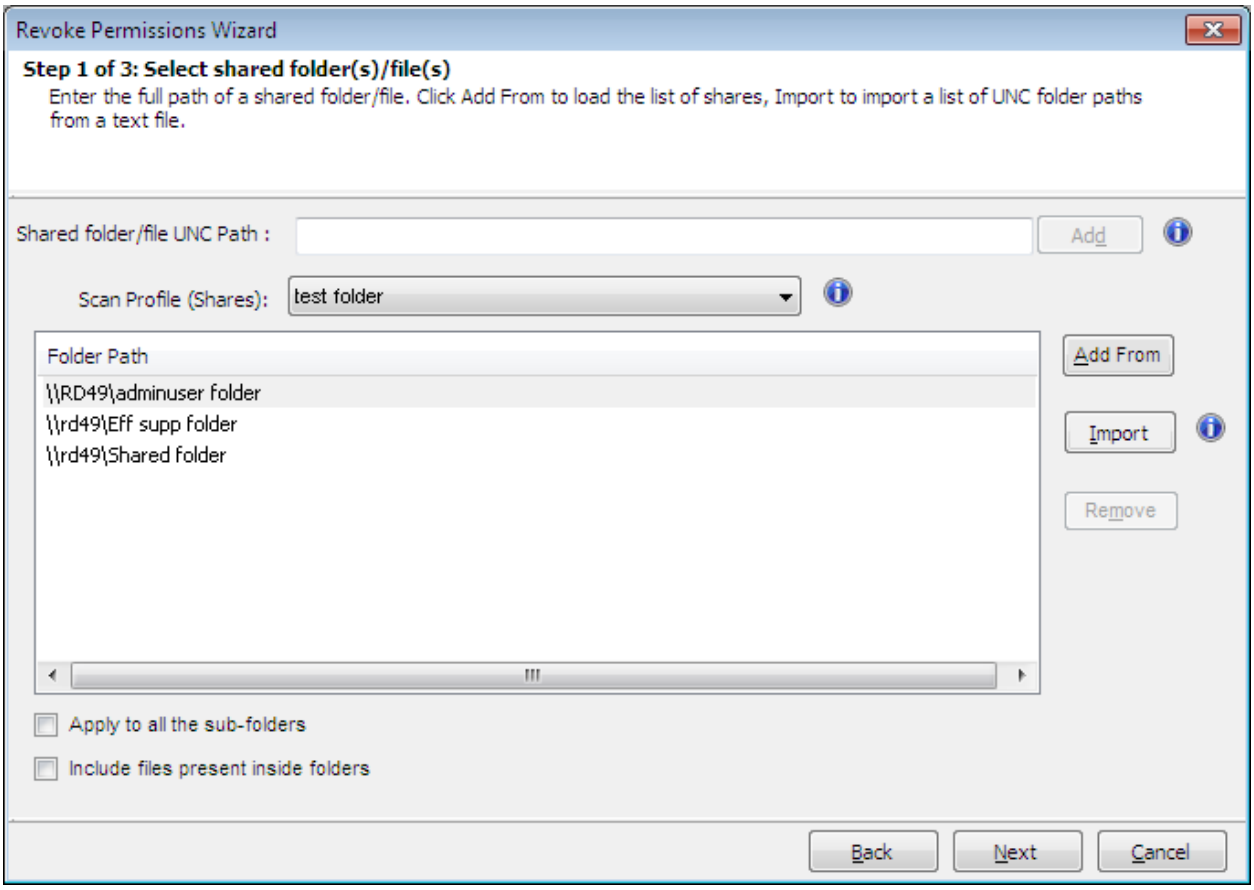
Select shared folder(s)/file(s) by using any of the input options displayed.


Revoke Permissions Wizard
Step 1 of 3: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Shared folder/file UNC Path :
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Apply to all the sub-folders
Include files present inside folders
Back
Next
Cancel

- Click the option **Add From**
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use **Select a Scan Profile (Shares)** option to use the Shares added in the profile.

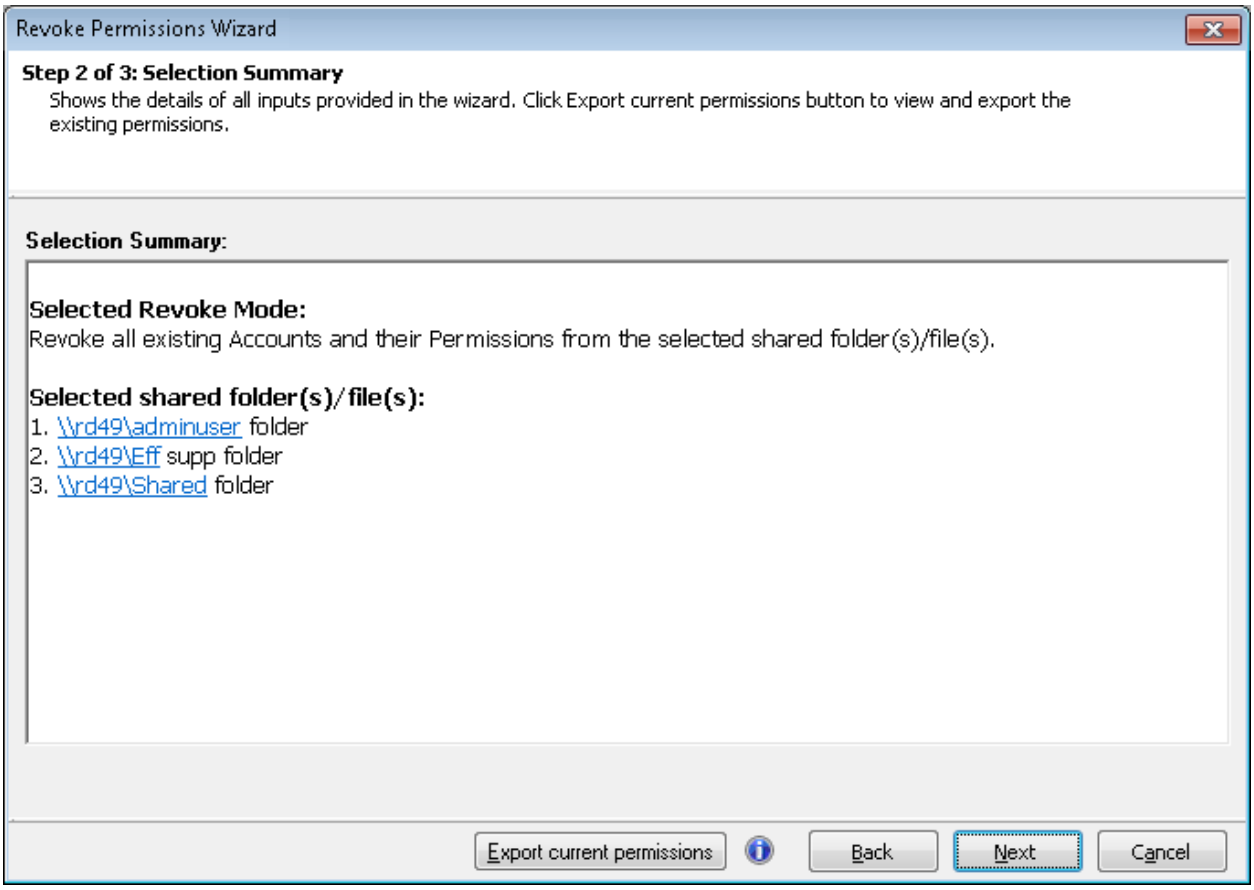

Revoke Permissions Wizard
Step 1 of 3: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Shared folder/file UNC Path :
Add
Scan Profile (Shares):
test folder
Folder Path
\\RD49\adminuser folder
\\rd49\Eff supp folder
\\rd49\Shared folder
Add From
Import
Remove
Apply to all the sub-folders
Include files present inside folders
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to share list from a text file by using the **Import** button.

Click **Next** to proceed to the Next step.

Step 3: Selection Summary

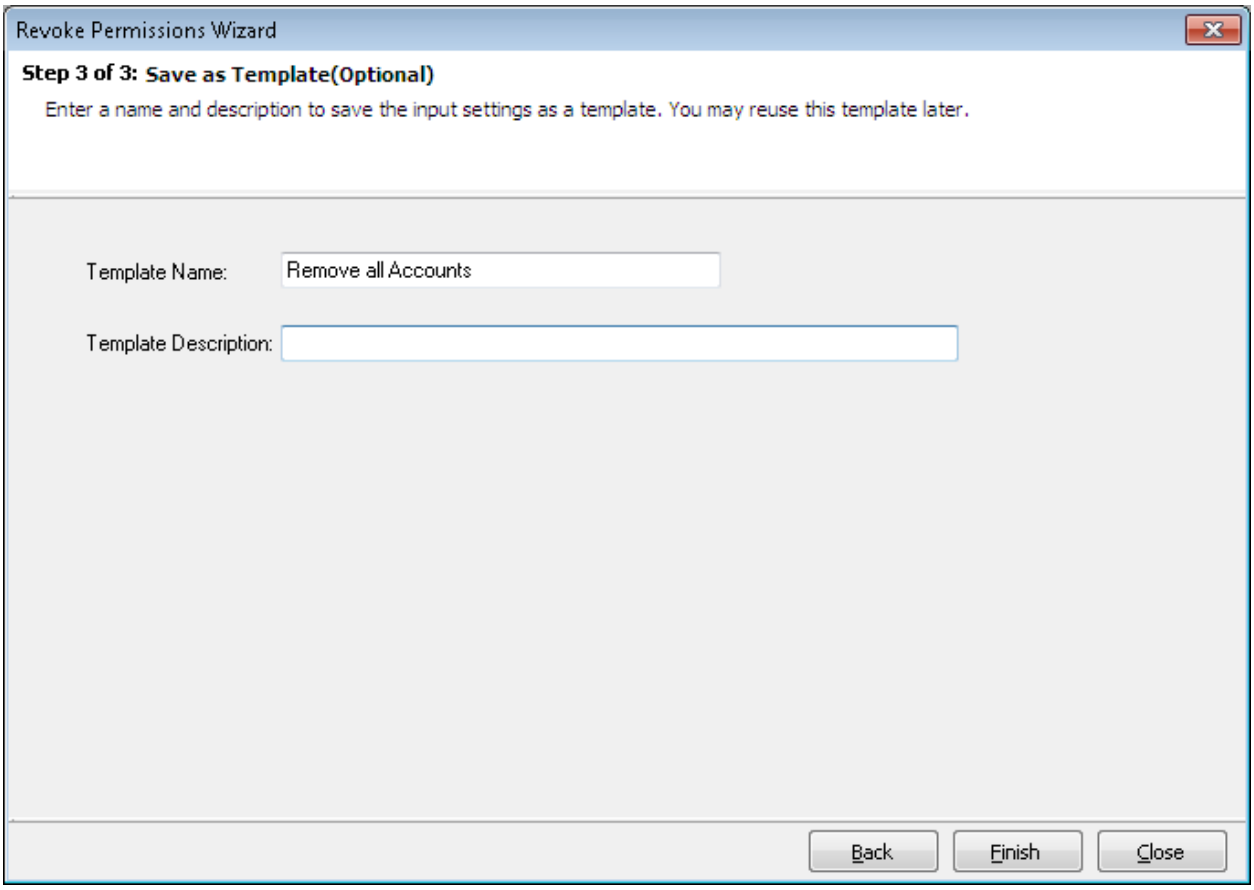
This step displays the summary of data selected to Revoke permissions and you can also view and export the existing permissions before changes are applied, by clicking on the Export current permissions button.


Revoke Permissions Wizard
Step 2 of 3: Selection Summary
Shows the details of all inputs provided in the wizard. Click Export current permissions button to view and export the existing permissions.
Selection Summary:
Selected Revoke Mode:
Revoke all existing Accounts and their Permissions from the selected shared folder(s)/file(s).
Selected shared folder(s)/file(s):
1. \\rd49\adminuser folder
2. \\rd49\Eff supp folder
3. \\rd49\Shared folder
Export current permissions
Back
Next
Cancel

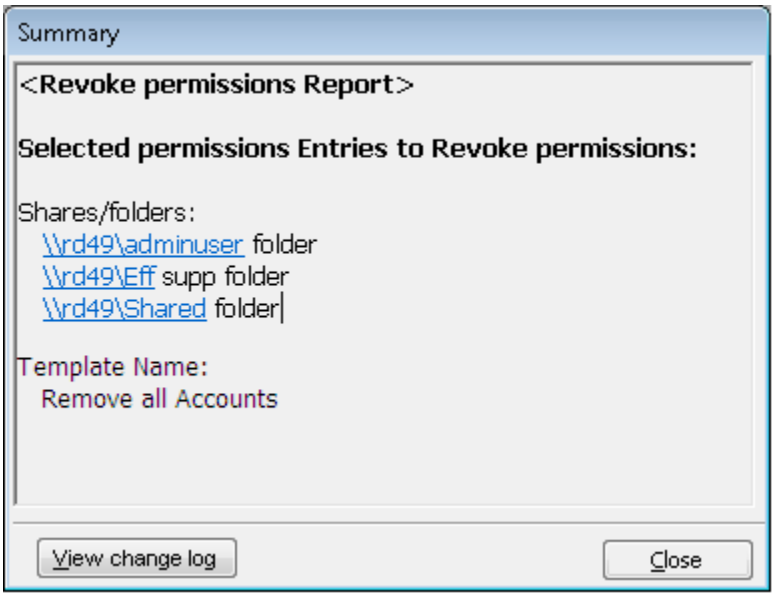
Click **Next** to proceed to the Next step.

Step 4: Save as template

Enter a name and description to save these settings as a template to reuse later.

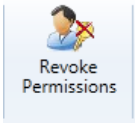

Revoke Permissions Wizard
Step 3 of 3: Save as Template(Optional)
Enter a name and description to save the input settings as a template. You may reuse this template later.
Template Name:
Remove all Accounts
Template Description:
Back
Finish
Close

Click **Finish** to complete the Grant Permissions task. After the Revoke permissions action completed, the summary of all the input data would shown below along with the option "View changelog" to view the summary of all the input data and task completion status.



How to revoke the exact matching permissions from the shares permissions?

The Revoke Permissions feature provides an option to revoke selected accounts and their permissions, only if the selected permission entries match exactly with the ACE entries in the shares permissions list.

Click on 

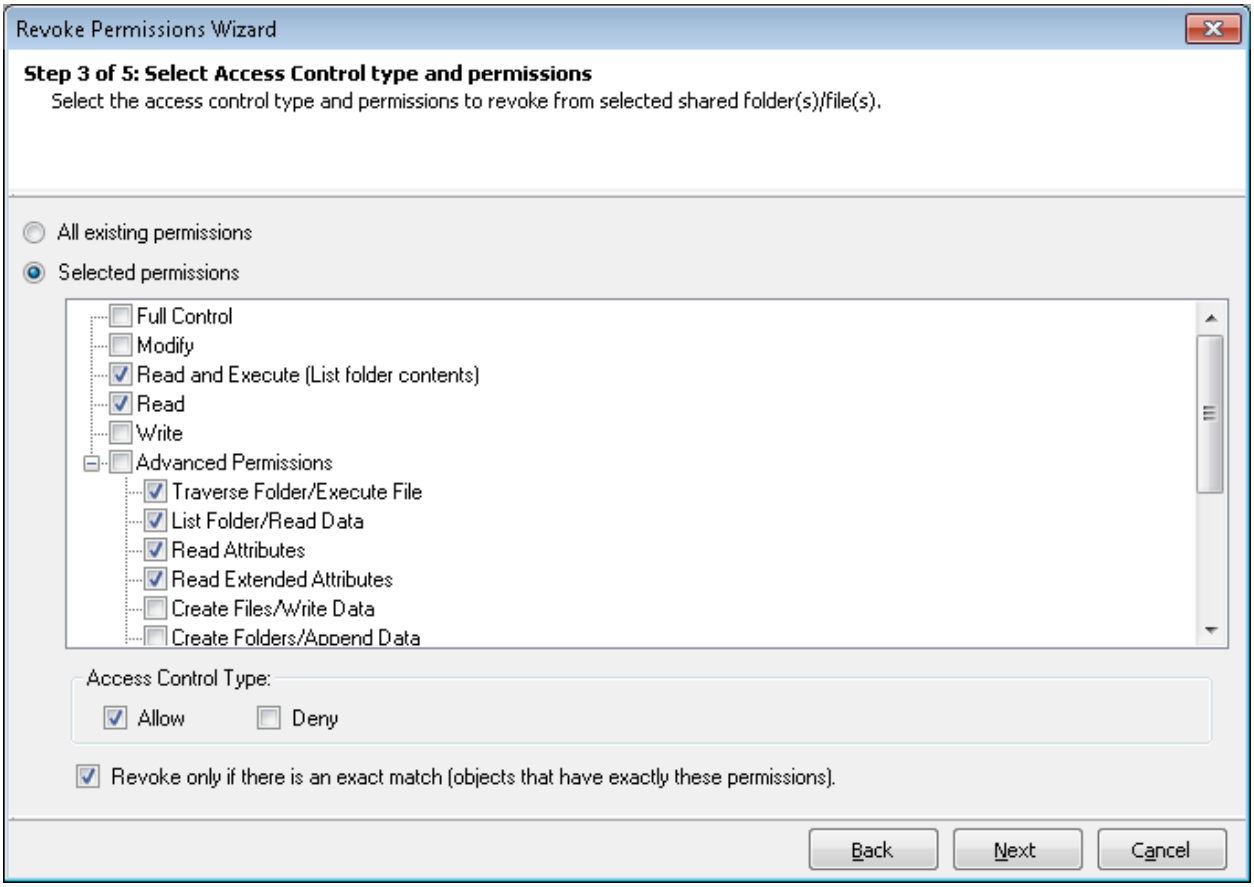
button.

The Revoke Permissions window will be displayed.

- Follow the steps 1 through 3 as outlined in How to Revoke Permissions from selected shares permissions list?

Step 4: Select Access Control type and permissions

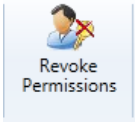
Select ACE type and permissions and also check the option **Revoke only if there is an exact match**



- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Revoke Permissions from selected shares permissions list?

How to revoke the selected accounts and all their permissions from the share permissions list?

The **Revoke Permissions** feature provide the option to remove the selected accounts and all their permissions from the share permissions list.

Click on 

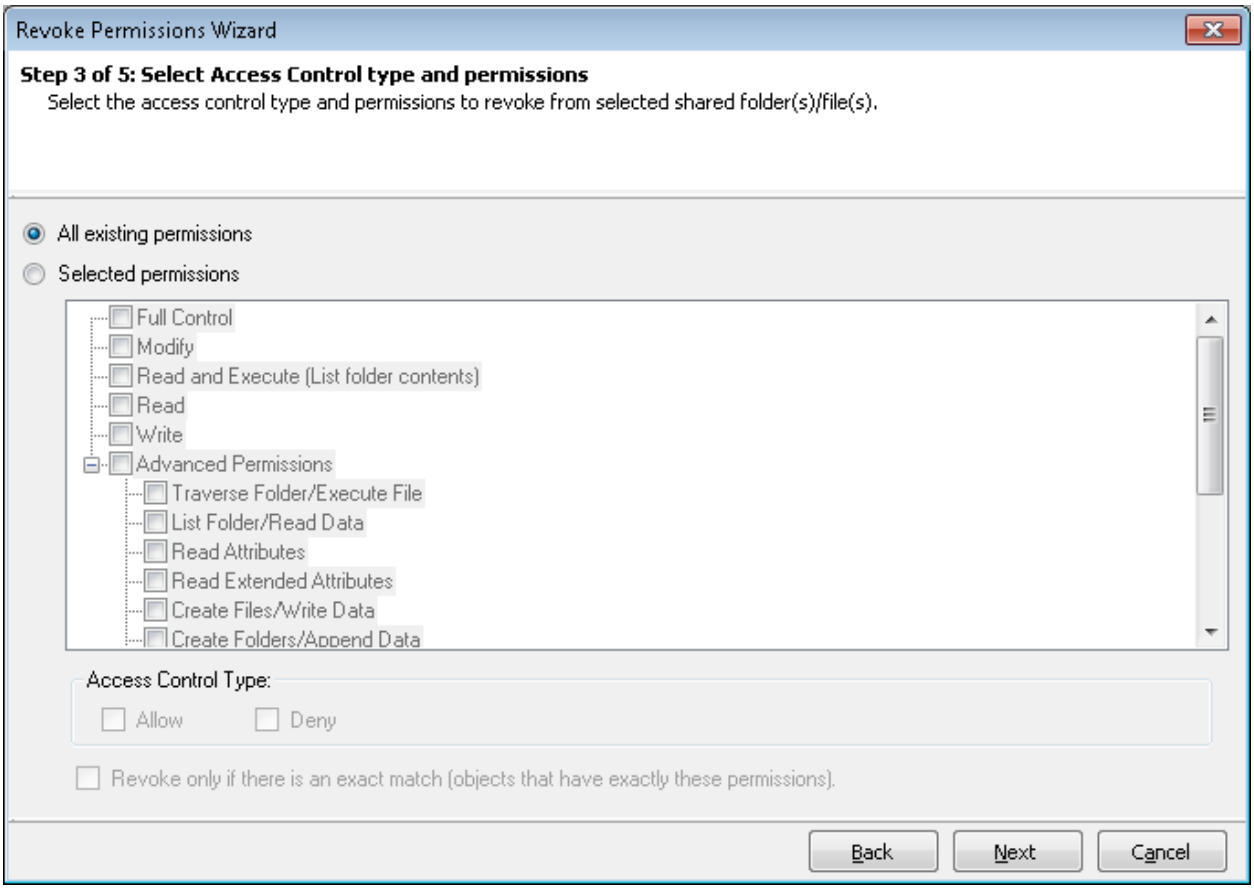
button.

The Revoke Permissions window will be displayed.

- Follow the steps 1 through 3 as outlined in How to Revoke Permissions from selected Shares permissions list?

Step 4: Select Access Control type and permissions

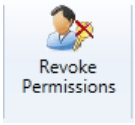
Select the option **All existing permissions**



- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Revoke Permissions from selected Shares permissions list?

How to revoke the Orphaned SIDs from the share permissions list?

The **Revoke Permissions** feature allows an option to revoke Orphaned SIDs from the share permissions list.

Click 

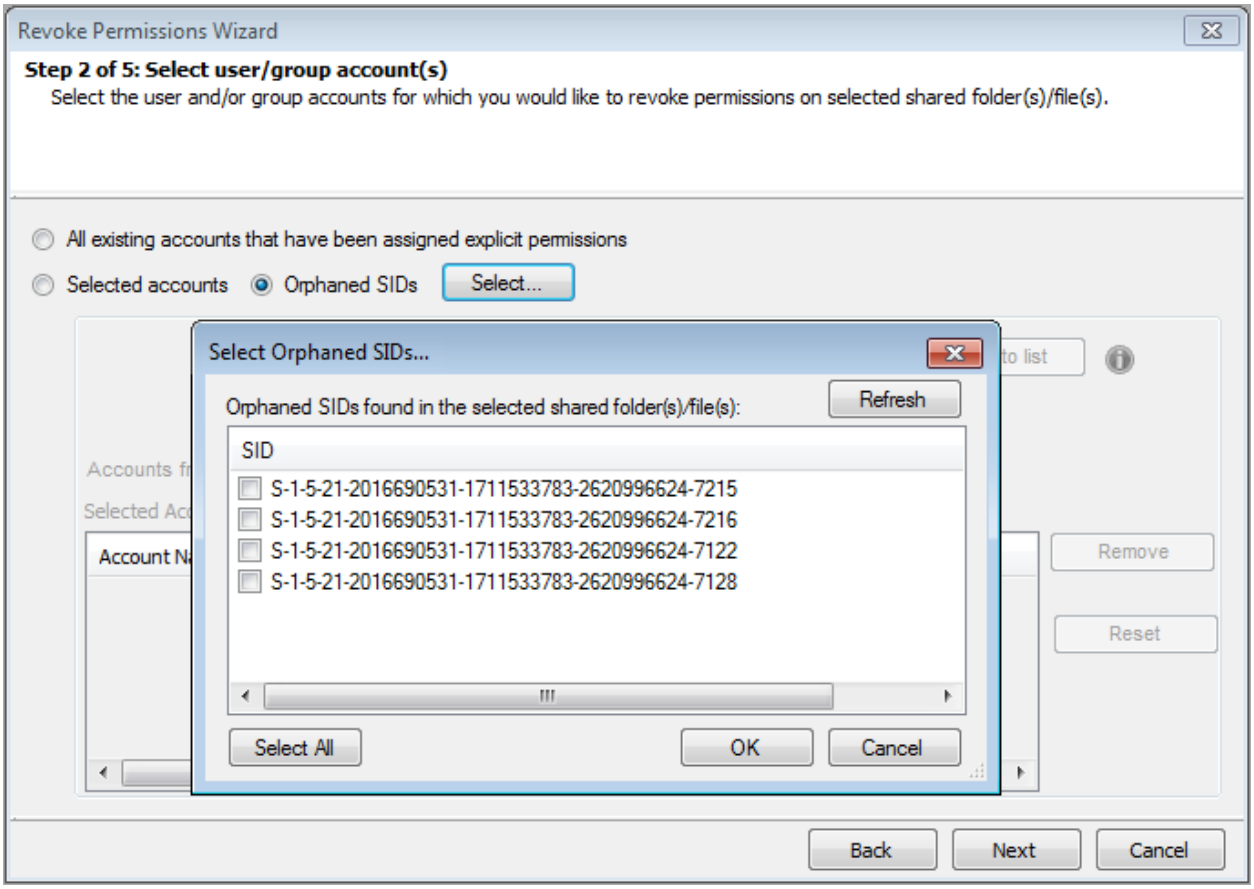
button.

The Revoke Permissions window will be displayed.

- Follow the steps 1 through 2 as outlined in How to Revoke permissions from the selected shares permissions list?

Step 3: User and/or Group selection

Select the **Orphaned SIDs** option and click **Select...** button.

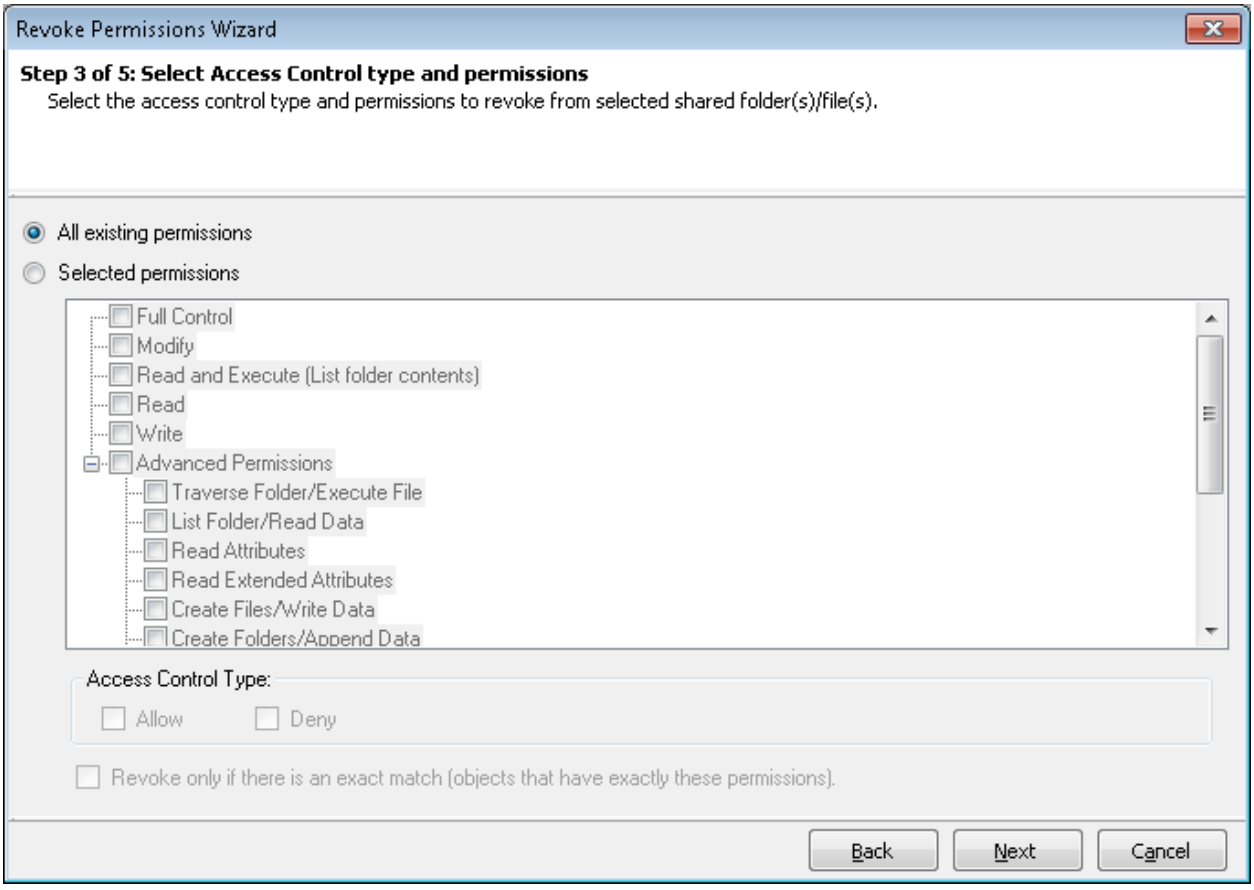


Select the Orphaned SIDs in **Select Orphaned SIDs...** dialog. Once SID selection is complete, click OK.

Click **Next** to proceed to the next step.

Step 4: Select Access Control type and permissions

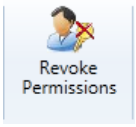
Click **All existing permissions** option.



- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in [How to Revoke Permissions from selected Shares permissions list?]

How to revoke permissions from the selected shares permissions list?

The **Revoke Permissions** feature provides many options to remove accounts and their permissions from the existing list of ACE entries in shared folders and files. You may revoke all existing explicit accounts and also you may selectively revoke a set of permissions granted to accounts.

Click on 

button.

The Revoke Permissions window will be displayed as shown below:

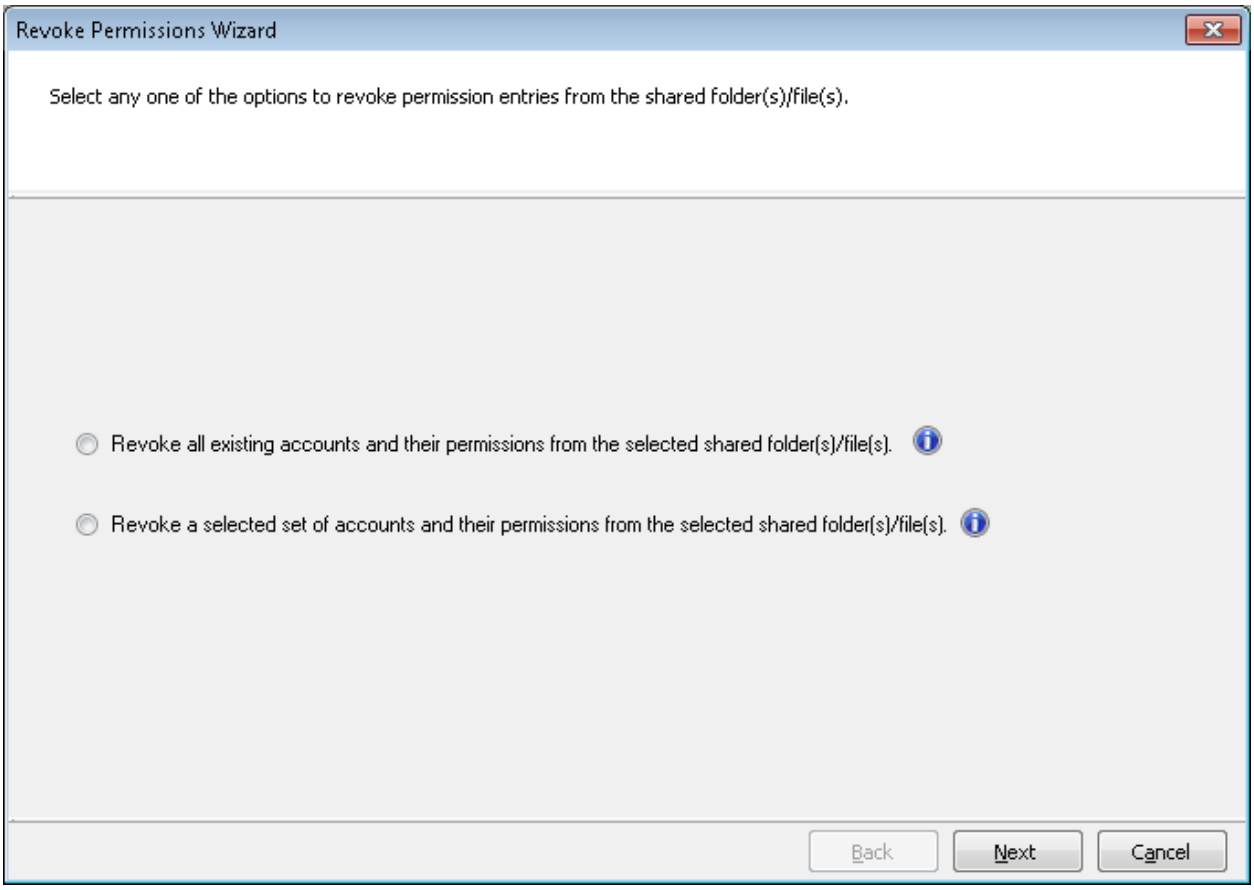
Step 1: Select a Revoke permissions option

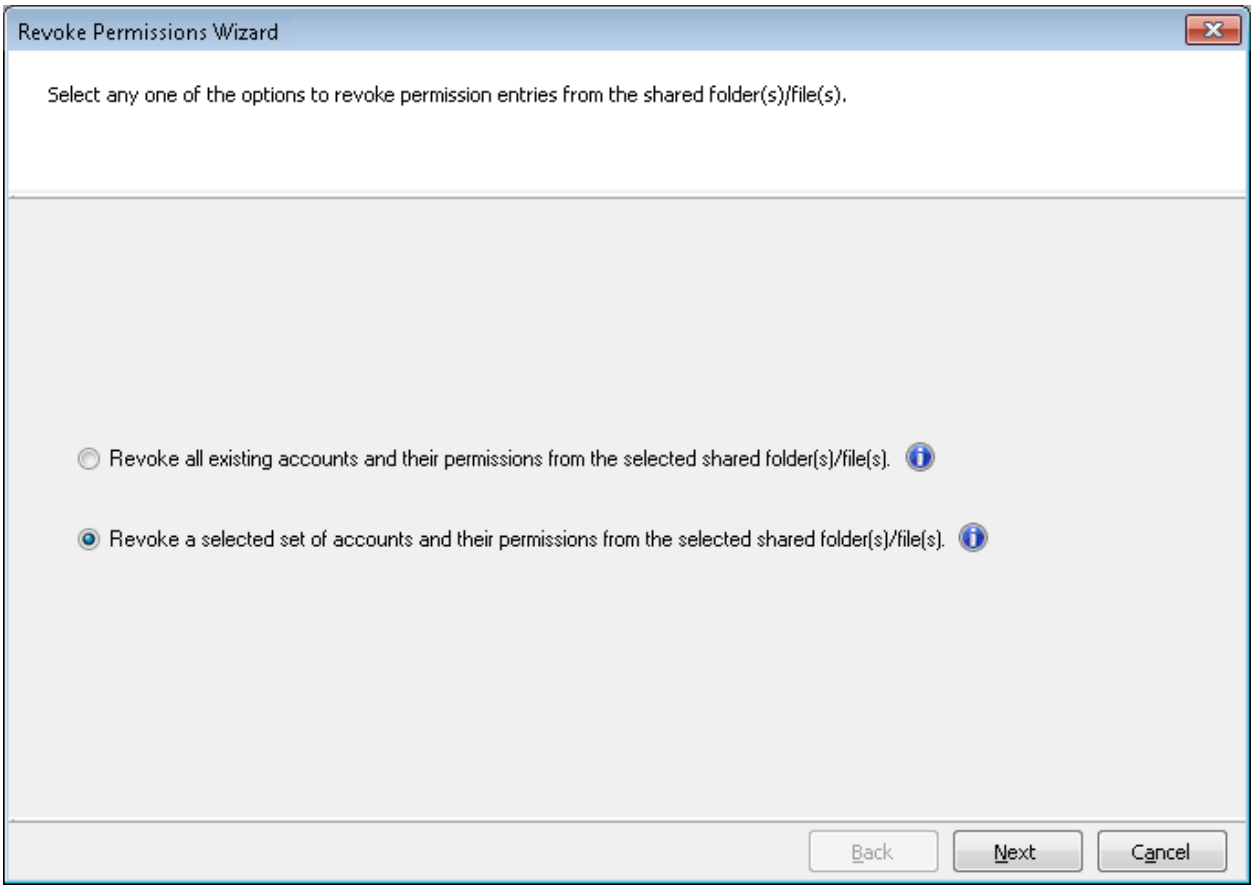
Select any one of the following options:

- **Revoke all existing accounts and their permissions from the selected shared folder(s)/file(s)**: This option will remove **all explicitly assigned accounts** with all their permissions from the selected shared folder(s)/file(s) permissions list.

  Note: This will not affect the accounts which are inherited from the parent of the current object. If you still wish to break the inheritance from the parent object, you may use the Grant Permissions or Modify Permissions tool to block inheritance.

- **Revoke a selected set of accounts and their permissions from the selected shared folder(s)/file(s)**: This option will revoke the selected accounts and their permissions from the shared folder(s)/file(s) permissions list. In this option, you can selectively revoke a set of permissions granted to accounts.

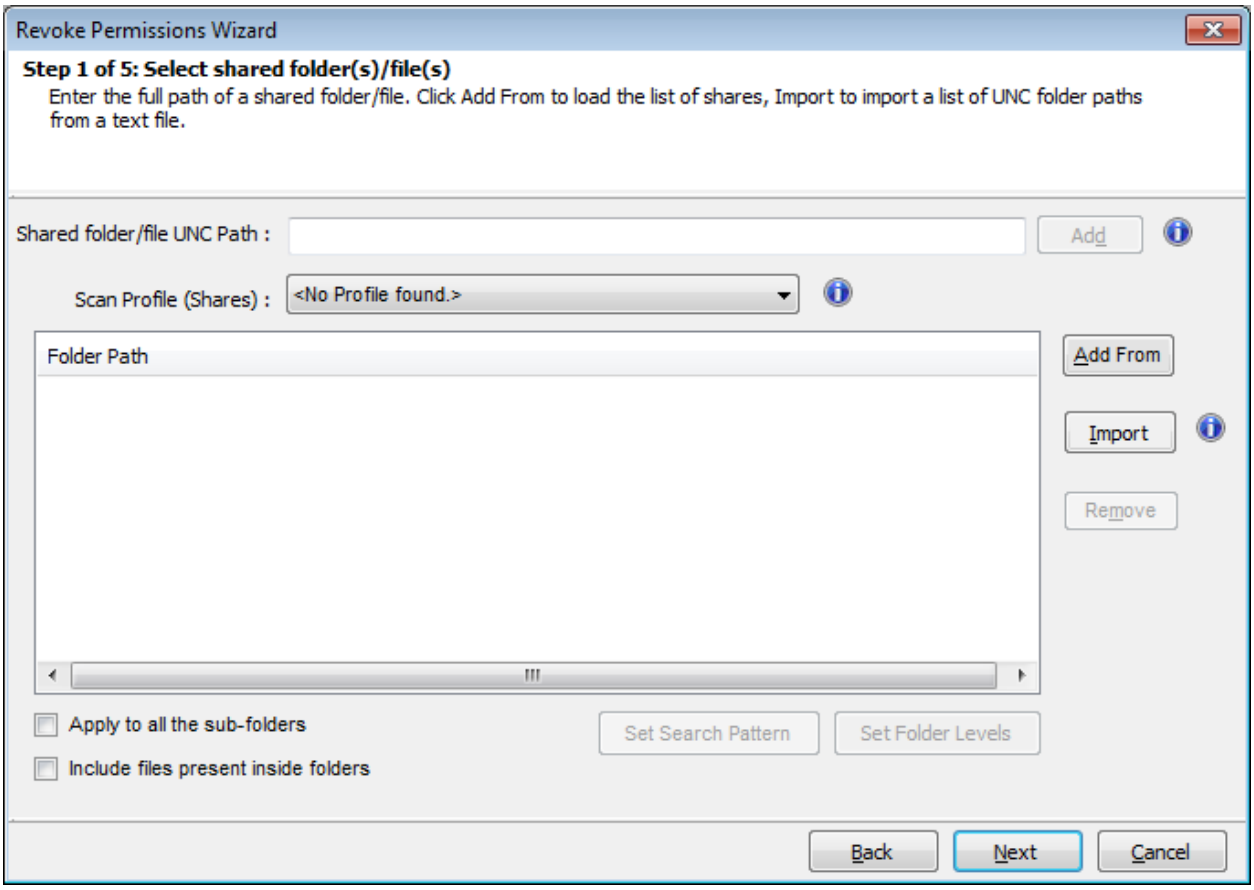

Revoke Permissions Wizard
Select any one of the options to revoke permission entries from the shared folder(s)/file(s).
Revoke all existing accounts and their permissions from the selected shared folder(s)/file(s).
Revoke a selected set of accounts and their permissions from the selected shared folder(s)/file(s).
Back
Next
Cancel


Revoke Permissions Wizard
Select any one of the options to revoke permission entries from the shared folder(s)/file(s).
Revoke all existing accounts and their permissions from the selected shared folder(s)/file(s).
Revoke a selected set of accounts and their permissions from the selected shared folder(s)/file(s).
Back
Next
Cancel

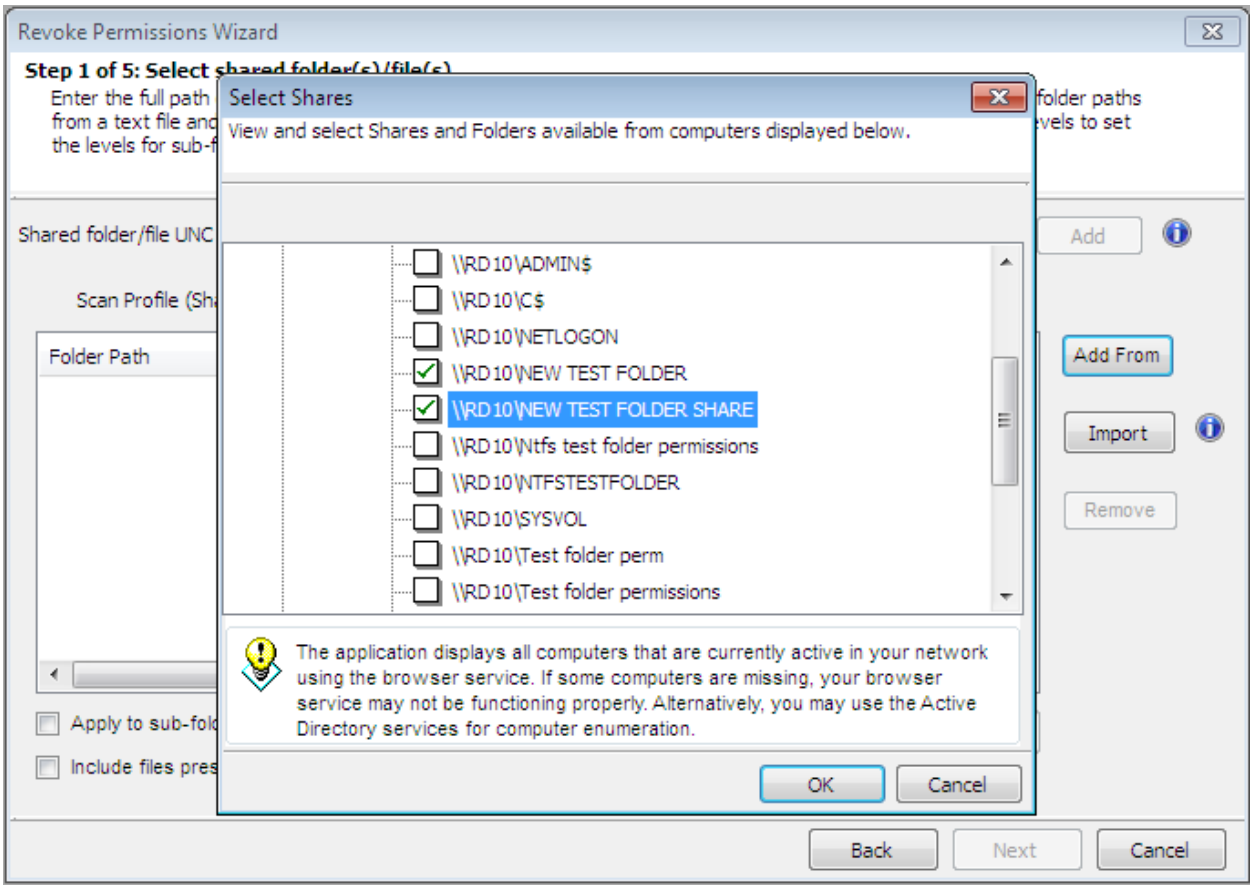
Click **Next** to proceed to the Next step.

Step 2: Select shared folder(s)/file(s)

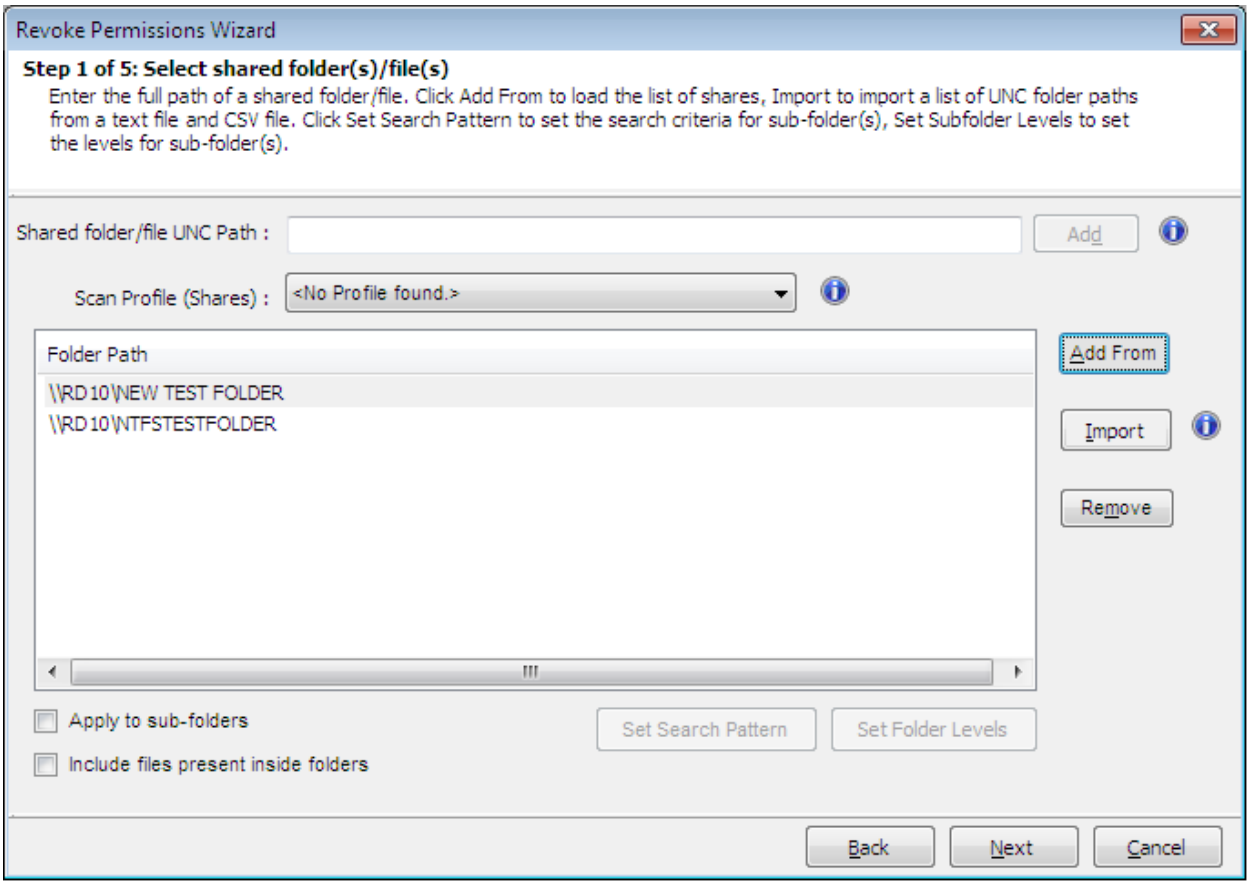
Select shared folder(s)/file(s) by using any of the input options displayed.


Revoke Permissions Wizard
Step 1 of 5: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Shared folder/file UNC Path :
Add
Scan Profile (Shares) :
<No Profile found.>
Folder Path
Add From
Import
Remove
Apply to all the sub-folders
Include files present inside folders
Set Search Pattern
Set Folder Levels
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click **Add From** option
- Select one or more servers to enumerate its shared folder(s)/file(s)

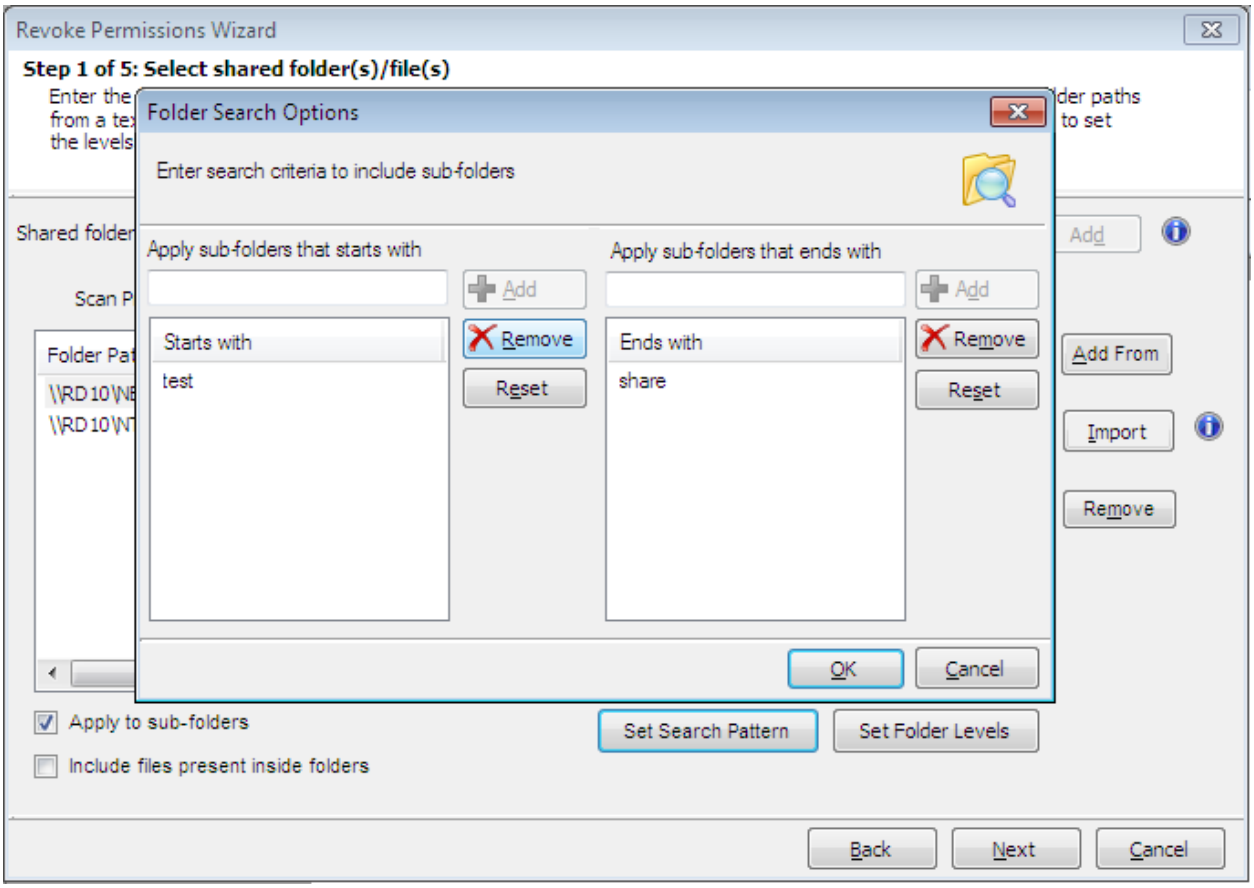


- Use **Select a Scan Profile (Shares)** option to use the Shares added in the profile.

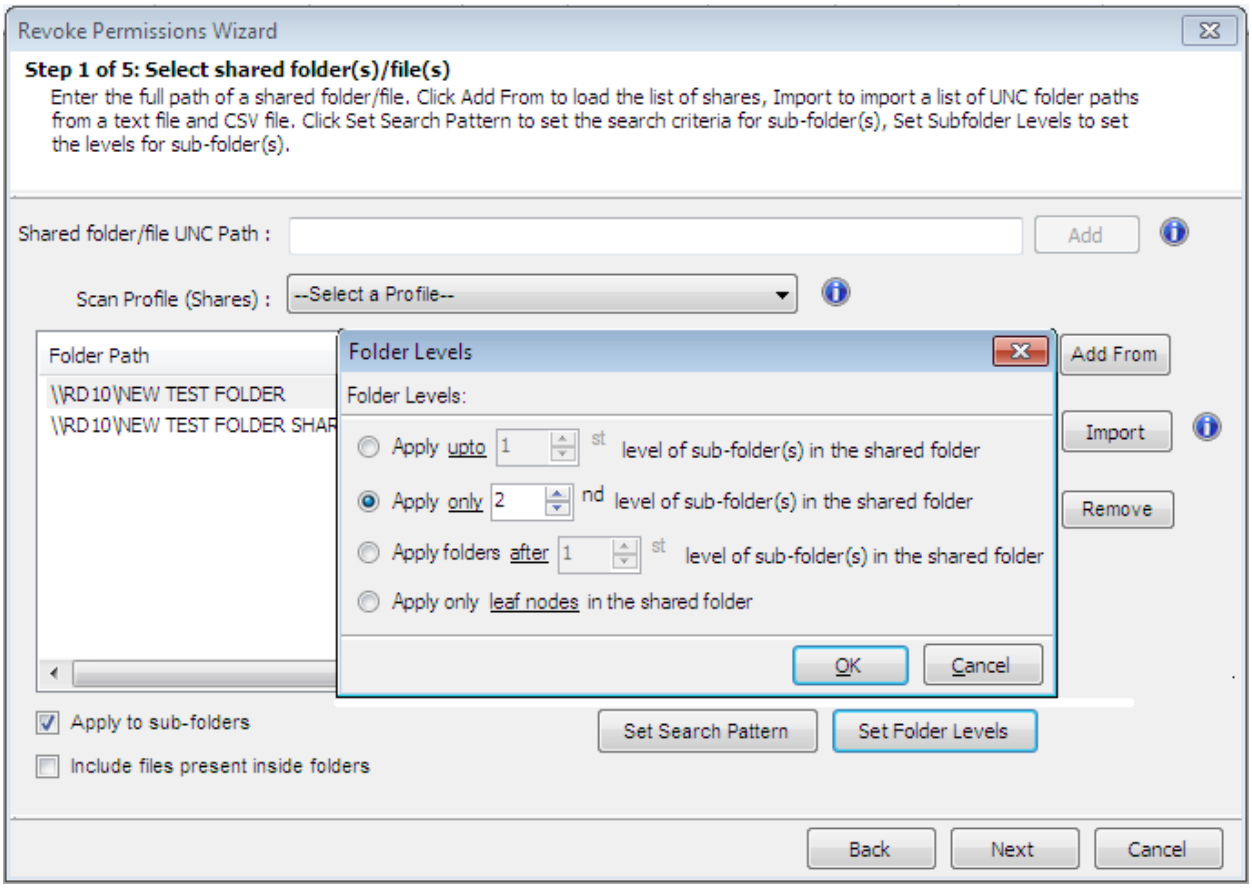

Revoke Permissions Wizard
Step 1 of 5: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Click Set Search Pattern to set the search criteria for sub-folder(s), Set Subfolder Levels to set the levels for sub-folder(s).
Shared folder/file UNC Path :
Add
Scan Profile (Shares) :
<No Profile found.>
Folder Path
\\RD10\NEW TEST FOLDER
\\RD10\NTFSTESTFOLDER
Add From
Import
Remove
Apply to sub-folders
Include files present inside folders
Set Search Pattern
Set Folder Levels
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

- **Apply to all the sub-folders**: This option will revoke permissions from all sub-folders of the folders added in this wizard.
- **Include files present inside folders**: This option will revoke permissions from all files present in the added folders and their sub-folders.
- Use **Set Search Pattern** option to revoke permissions from sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example: Folder name starts with test, Folder name ends with share.



- Use **Set Folder Levels** option to revoke permissions in the selected levels of sub-folder(s) in the shared folder.


Revoke Permissions Wizard
Step 1 of 5: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Click Set Search Pattern to set the search criteria for sub-folder(s), Set Subfolder Levels to set the levels for sub-folder(s).
Shared folder/file UNC Path :
Add
Scan Profile (Shares) :
--Select a Profile--
Folder Path
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHAR
Folder Levels
Folder Levels:
Apply upto 1 st level of sub-folder(s) in the shared folder
Apply only 2 nd level of sub-folder(s) in the shared folder
Apply folders after 1 st level of sub-folder(s) in the shared folder
Apply only leaf nodes in the shared folder
OK
Cancel
Add From
Import
Remove
Apply to sub-folders
Include files present inside folders
Set Search Pattern
Set Folder Levels
Back
Next
Cancel

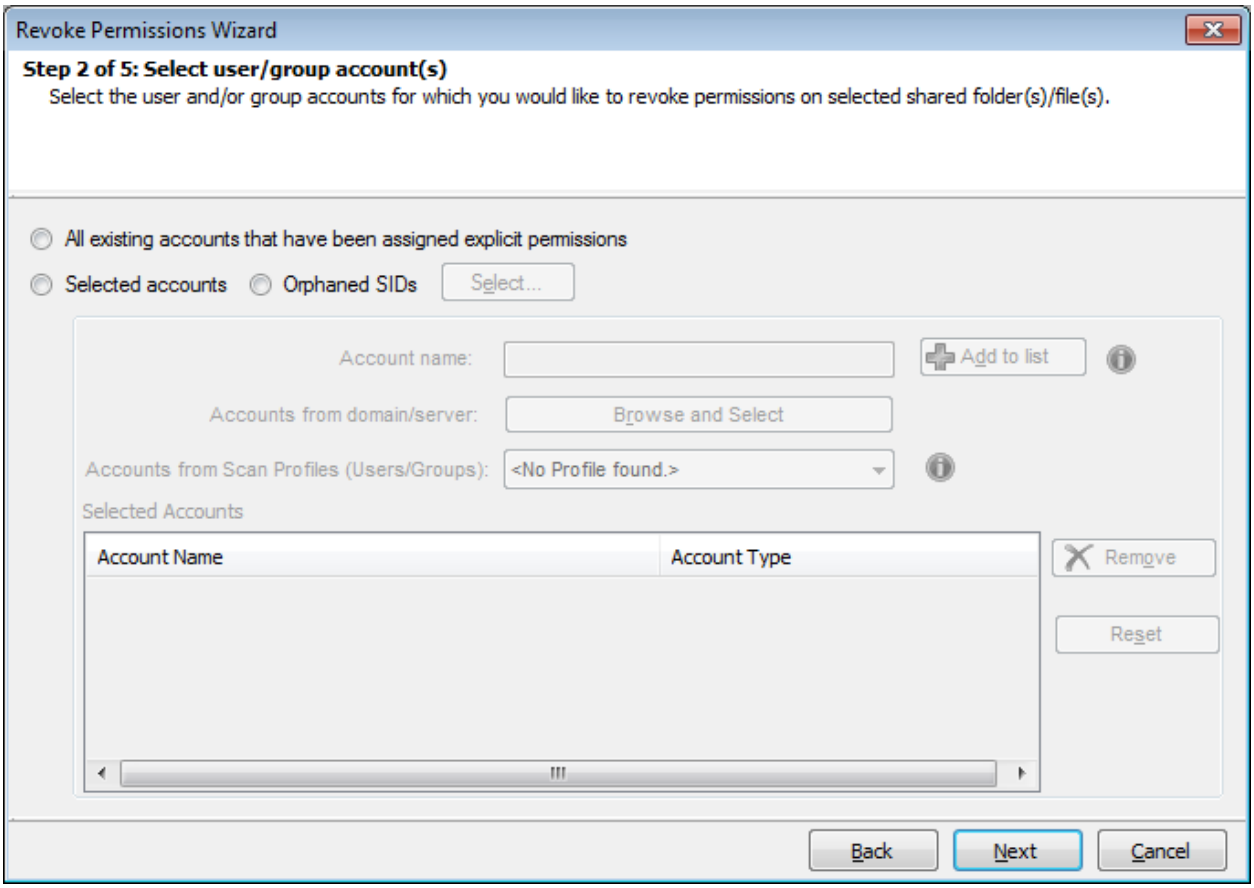
- **Apply upto N level(s) of sub-folder(s) in the shared folder:** This option will revoke permissions from sub-folders which are upto the specified folder traversal level.
- **Apply only Nth level of sub-folder(s) in the shared folder:** This option will revoke permissions from sub-folders which are in the specified folder level only.
- **Apply folders after N level(s) of sub-folder(s) in the shared folder:** This option will revoke permissions from sub-folders which are after the nth folder level of the selected folder.
- **Apply only leaf nodes in the shared folder:** This option will revoke permissions from the last child (leaf) nodes without affecting the parent folder's permissions.

Click **Next** to proceed to the Next step.

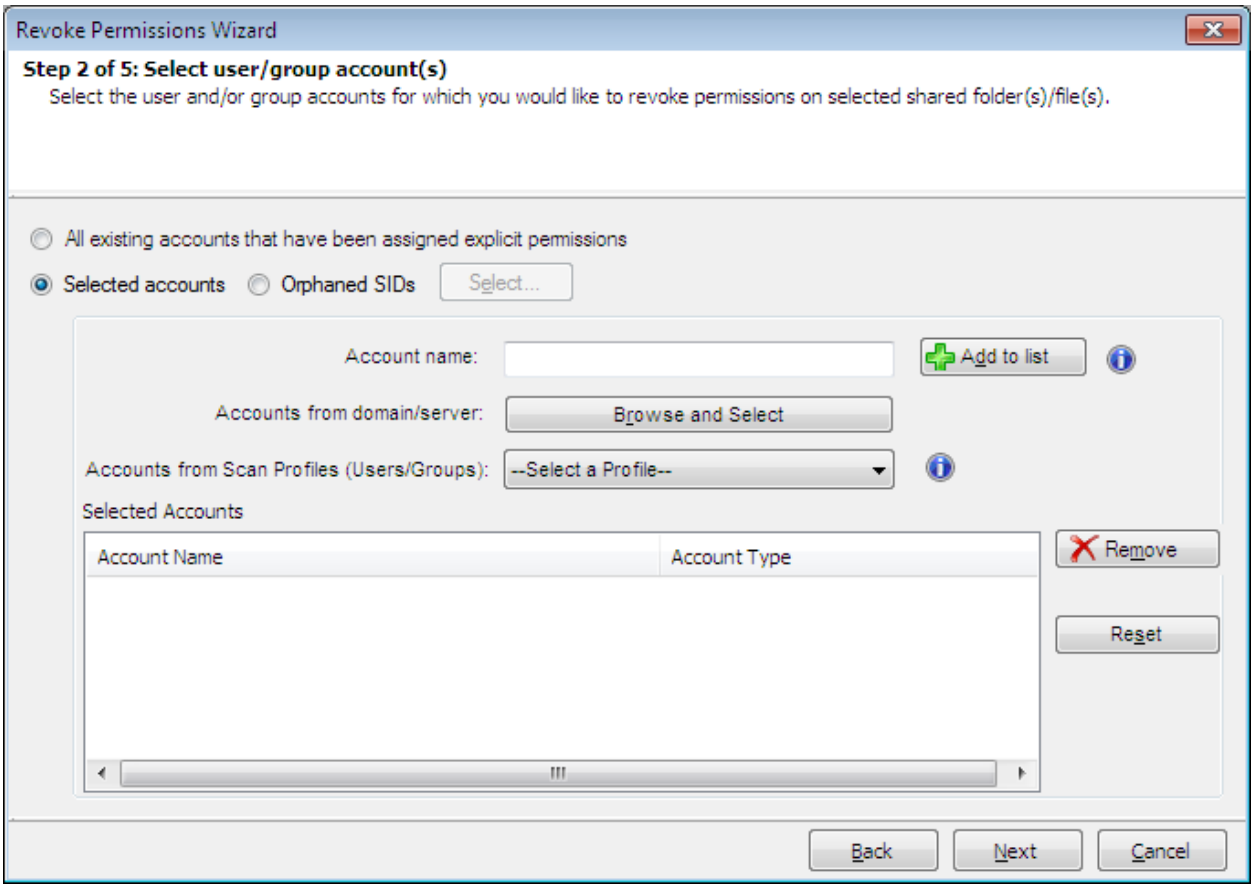
Step 3: Account Selection

You may select one of the account selection options below

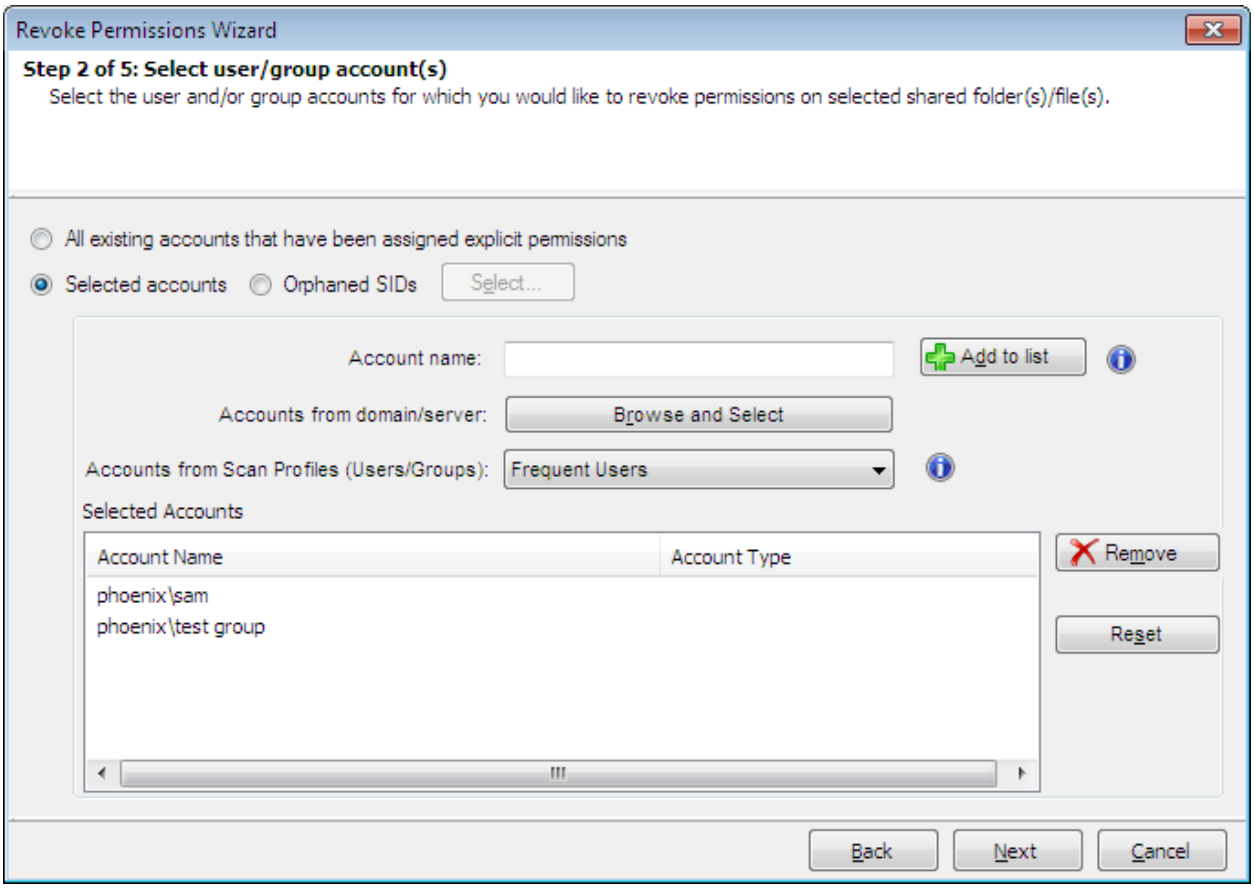
- **All existing accounts that have been assigned explicit permission**: This option will remove all the explicitly assigned accounts. It will not affect the accounts which are inherited from the parent of the current object.
- **Selected accounts**: This option will remove all or specific permissions for the selected accounts.



- Select the accounts, for which you wish to revoke permissions.
- The selected accounts will be added to the wizard as shown below:



- Use **Select a Scan Profile (Users/Groups)** option to use the accounts added in the profile.

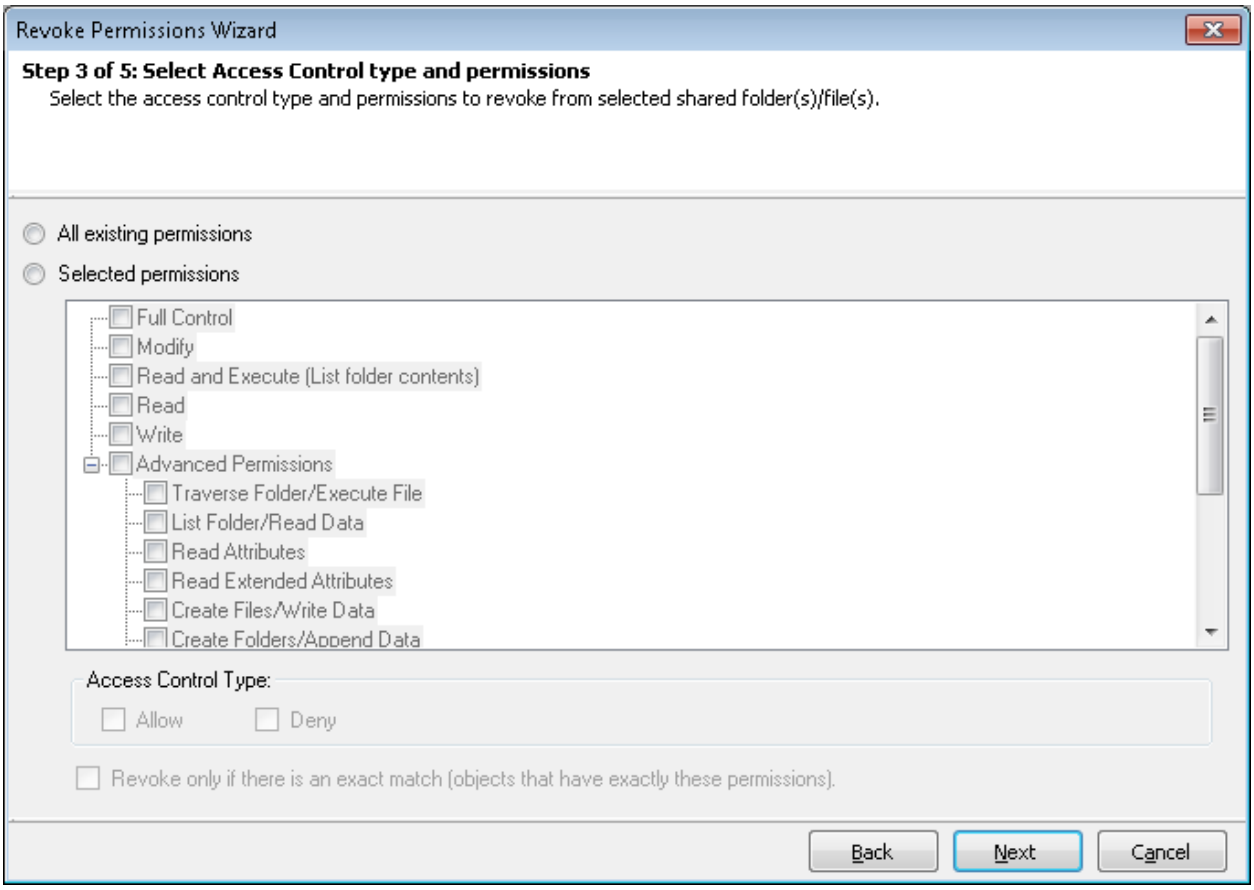


Click **Next** to proceed to the next step.

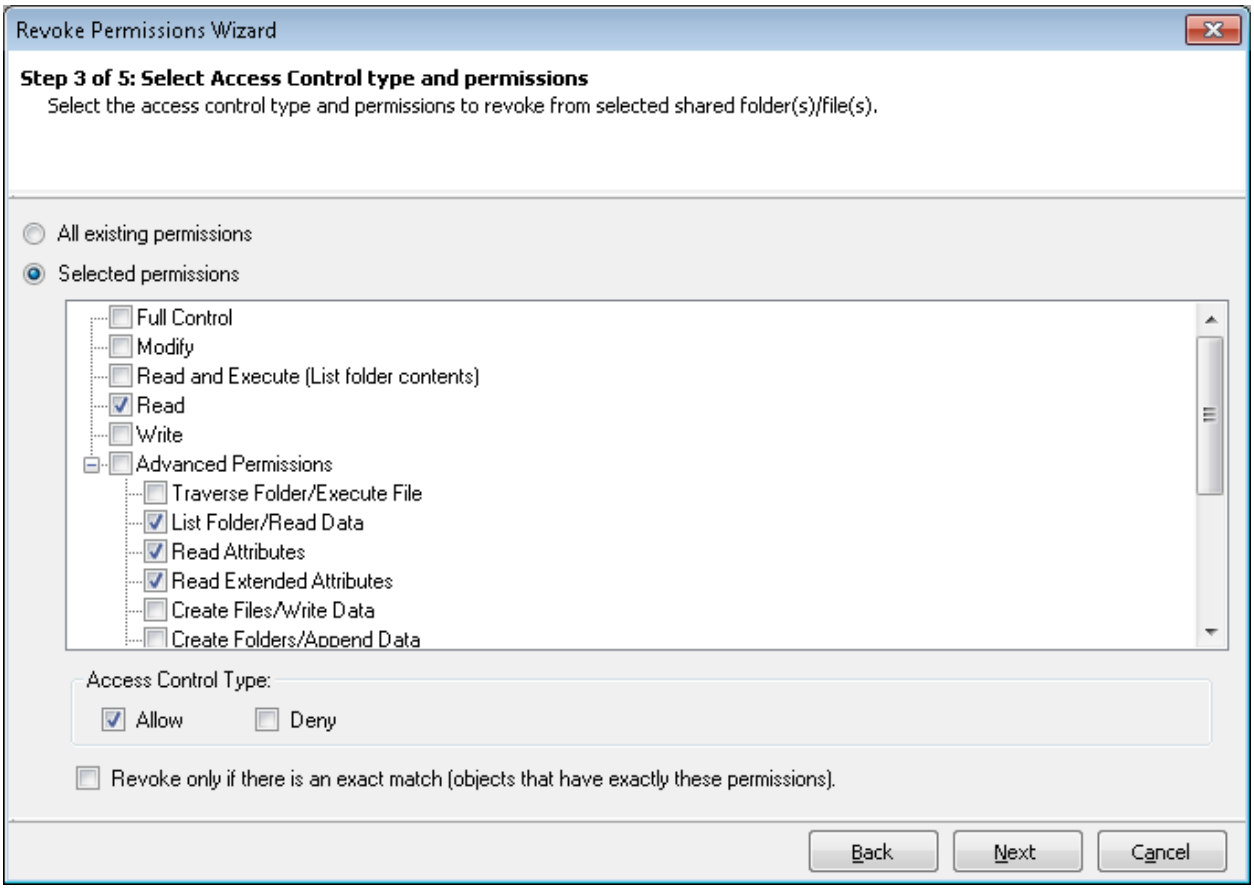
Step 4: Select Access Control type and permissions

You may select one of the options below:

- **All existing permissions**: This option will remove all existing permissions with accounts from the selected shared folder(s)/file(s) permissions list.
  Example: If the Account has many permissions like Allow type Read, Write, Take ownership and Deny type Modify, selecting this option will remove all the Allow and Deny permissions.
- **Selected permissions**: This option will remove only the selected permissions from the selected shared folder(s)/file(s) permissions list.
  Example: If the Account has the permissions Allow Read and Write and if Allow Read permission has been selected to revoke permissions, then this option will remove only Allow Read permissions from the permissions list and the remaining Write permissions will exist in the permissions list.
- **Revoke only if there is an exact match**: This option will remove the accounts permissions only when the selected permissions match exactly with an accounts existing permissions.
  Example: If a share has some accounts with permission as Allow Read and some accounts with permission as Allow Read and Execute, selecting the Allow Read permissions to revoke will remove only the accounts that exactly has Allow Read permission.



Select ACE type and permissions to revoke the selected accounts on the selected shared folder(s) /files(s)



Click **Next** to proceed to the next step.

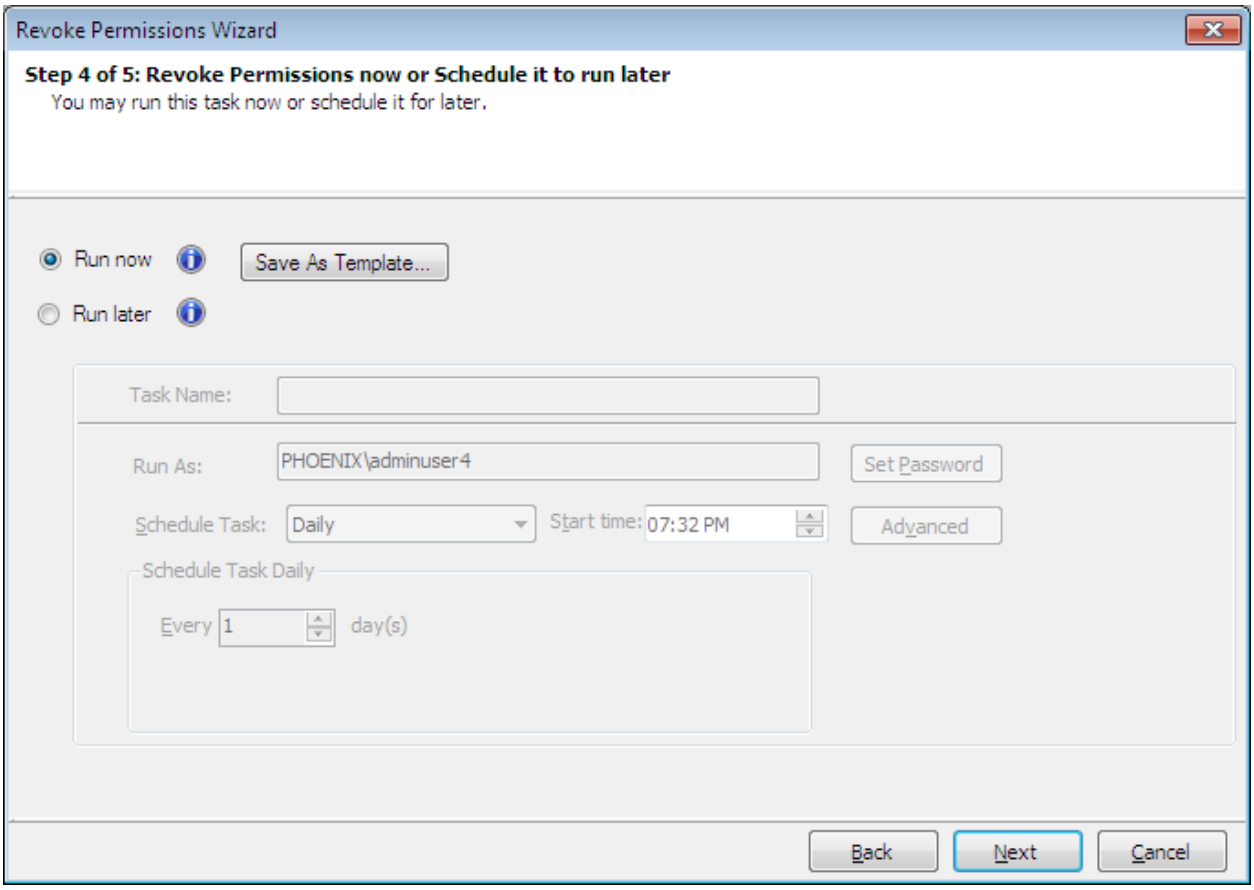
Step 5: Revoke permissions now or Schedule it to run later

You may use either Run now or Run later option.

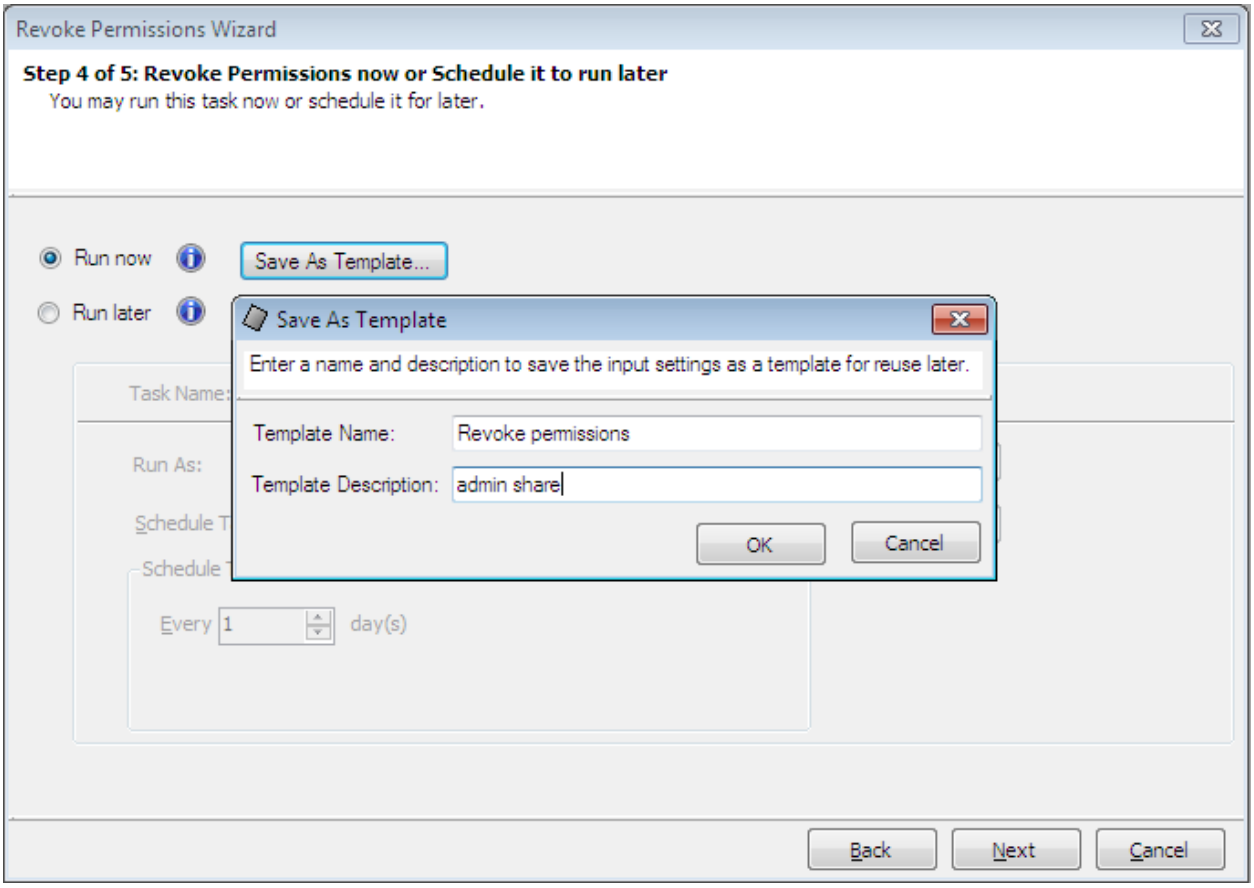
In Run now option, you can optionally save the input settings as a template. Click on **Save As Template**... and enter a name and description to save the wizard settings as a template for reuse.

In case of Run later option, enter a unique task name and specify its schedule settings.

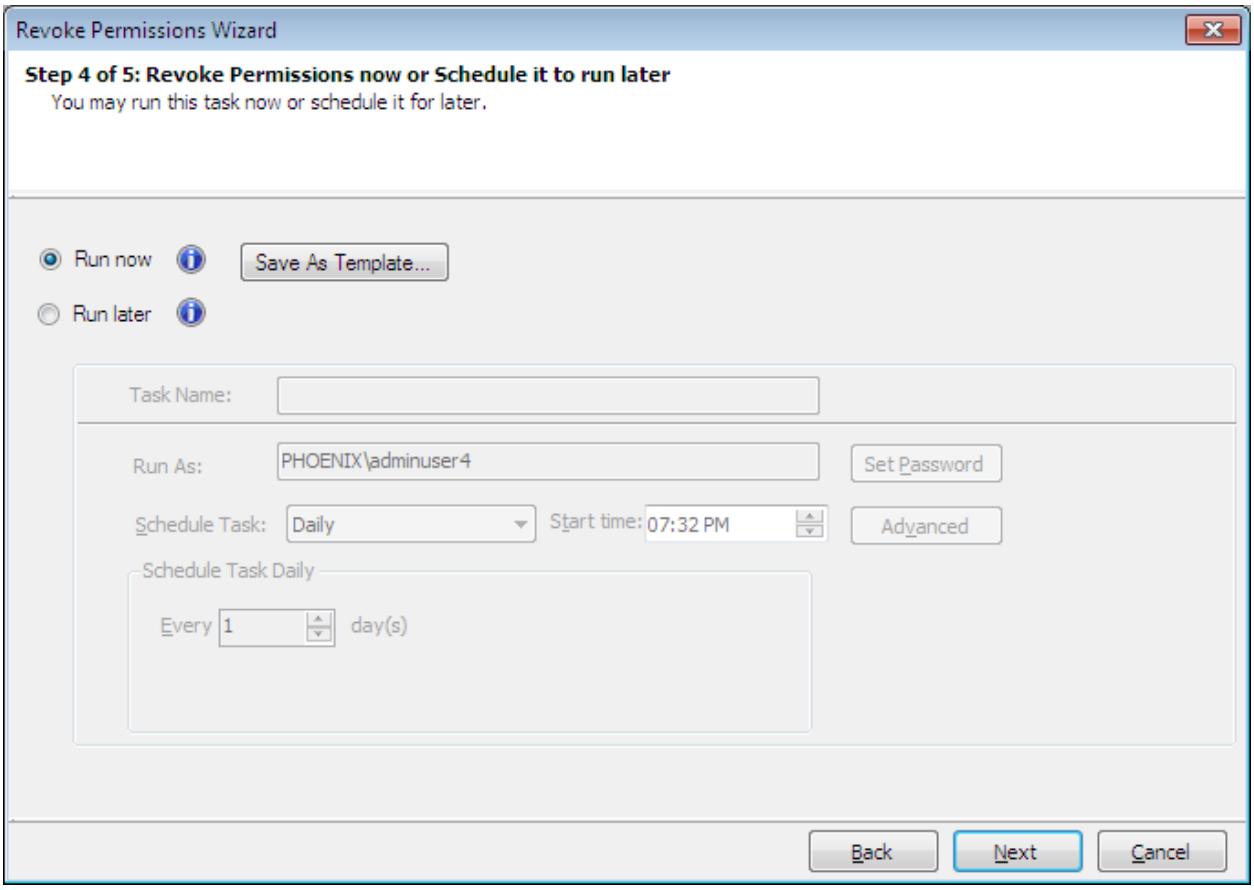
Select **Run now** option to run the task immediately after finishing the wizard steps.



In Run now option, you can optionally save the wizard settings by clicking on Save As Template... as shown below:



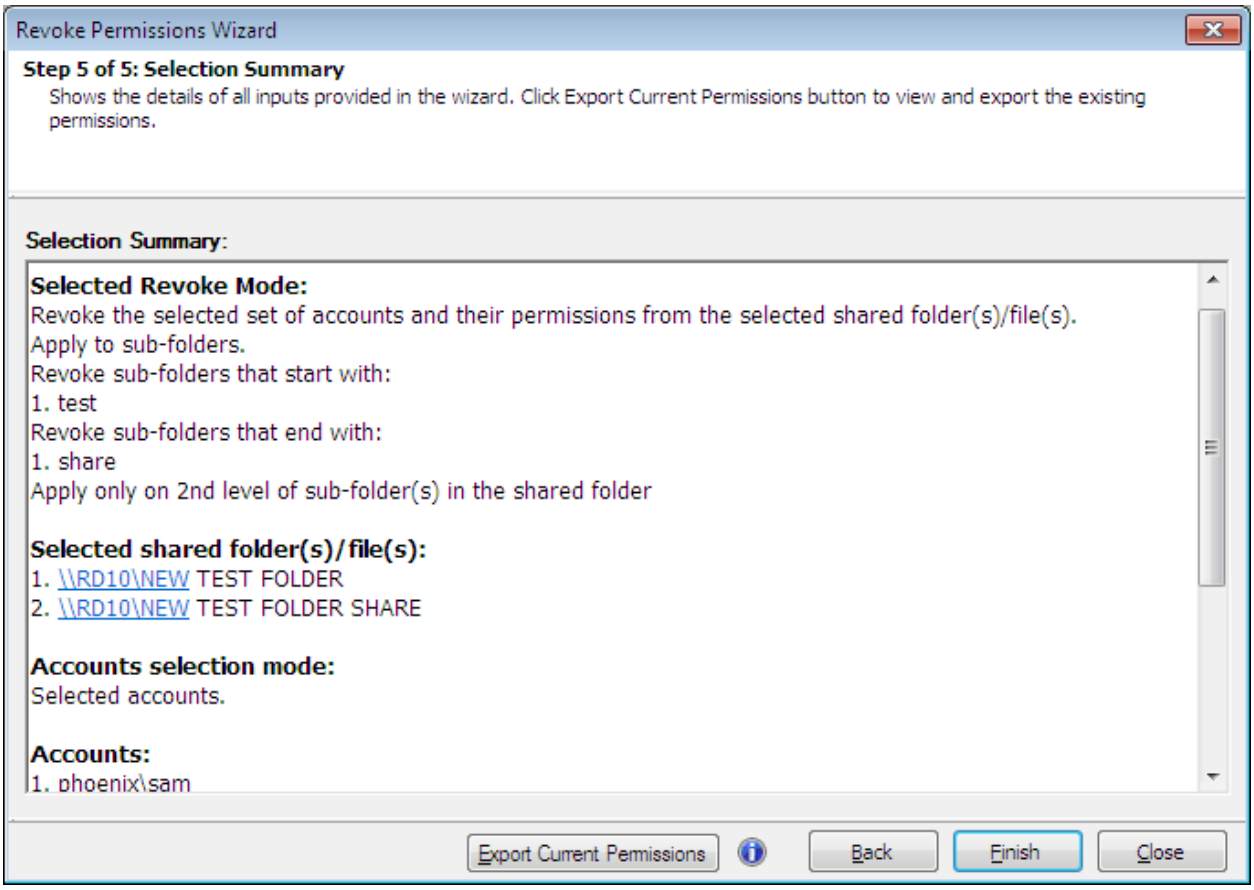
Click **OK** to save the input settings as a template.



Click Next to proceed to the next step.

Step 6: Selection Summary

This step displays the summary of data selected to Revoke permissions and you can also view and export the existing permissions before changes are applied, by clicking on the Export current permissions button.

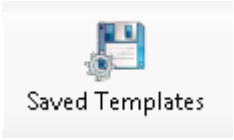

Revoke Permissions Wizard
Step 5 of 5: Selection Summary
Shows the details of all inputs provided in the wizard. Click Export Current Permissions button to view and export the existing permissions.
Selection Summary:
Selected Revoke Mode:
Revoke the selected set of accounts and their permissions from the selected shared folder(s)/file(s).
Apply to sub-folders.
Revoke sub-folders that start with:
1. test
Revoke sub-folders that end with:
1. share
Apply only on 2nd level of sub-folder(s) in the shared folder
Selected shared folder(s)/file(s):
1. \\RD10\NEW TEST FOLDER
2. \\RD10\NEW TEST FOLDER SHARE
Accounts selection mode:
Selected accounts.
Accounts:
1. phoenix\sam
Export Current Permissions
Back
Finish
Close

Click **Finish** to complete the Revoke Permissions wizard.

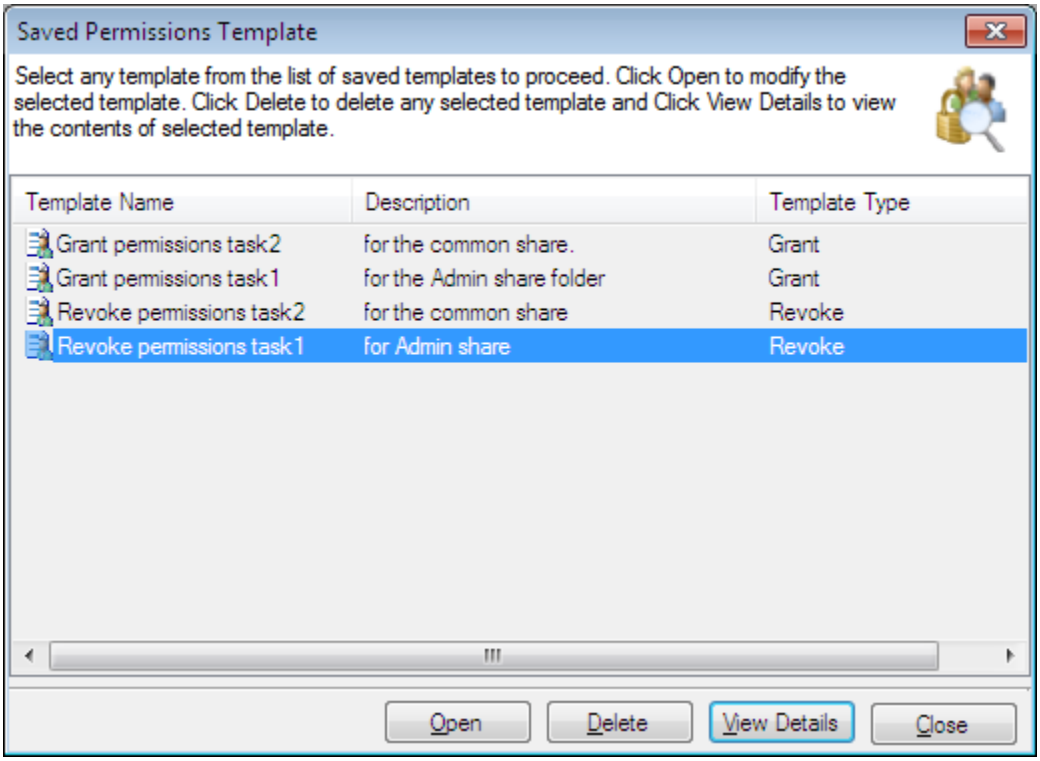
Permissions will be revoked as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.

How to reuse the Revoke Permissions template?

The Saved Templates contains the list of saved templates to Grant and Revoke permissions.

Click on 

button. The Saved Templates window will be displayed as shown below.



The saved templates window allows you to perform the following operations:

- Open an existing Template
- Delete a Template
- Preview the contents of a Template

Open an existing Template

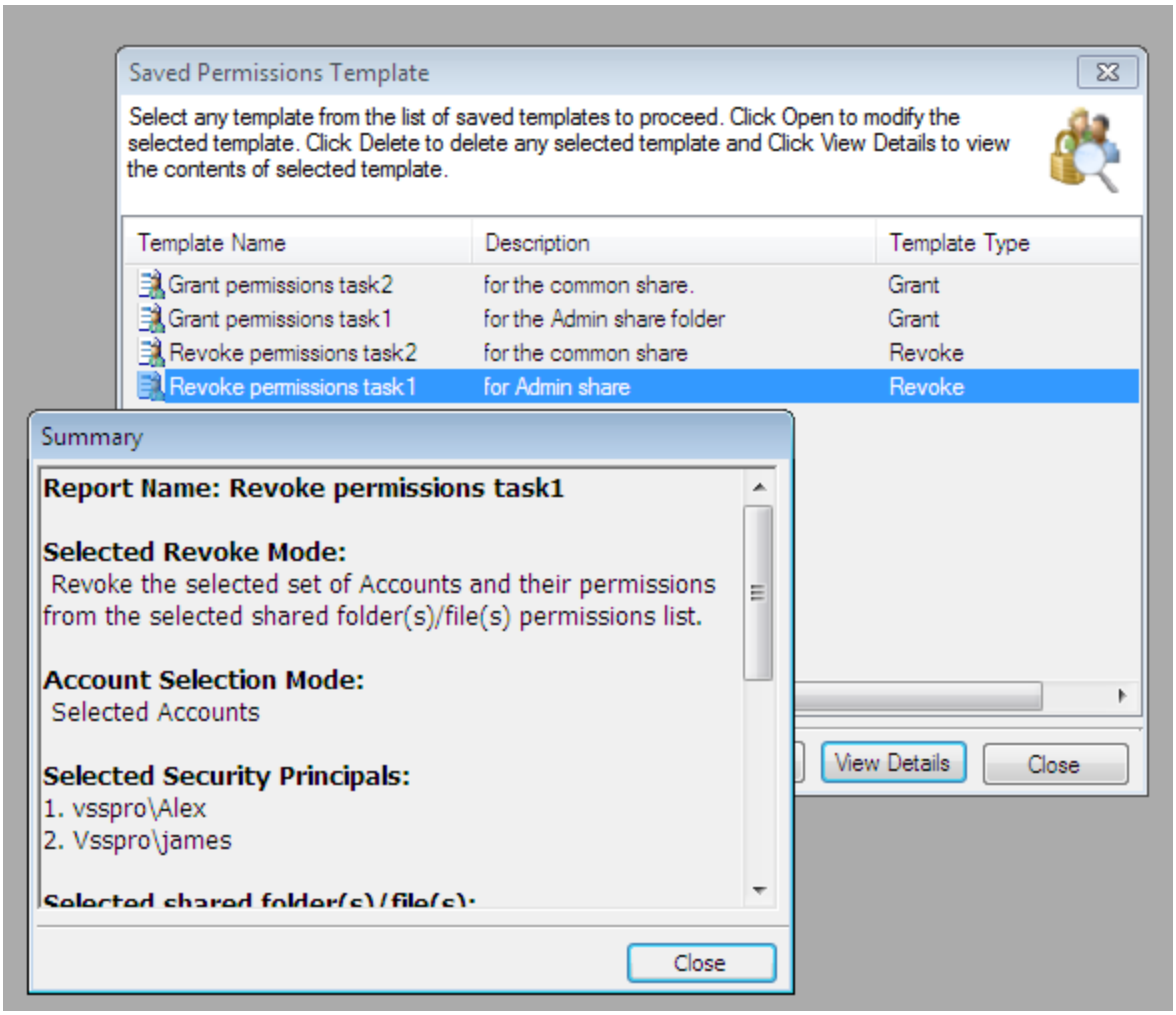
1. To open an existing Revoke permissions, select the Revoke permissions template and click Open button in the window. The Revoke permissions Dialog will appear on the screen which will allow you to edit the selected template.
2. During edit operation you can modify the computer list and permissions entries, however, you cannot modify the name of the template.

Delete a template

To delete a Revoke permissions template, select a Revoke permissions template which you want to delete, and then click Delete button. The selected template will be deleted permanently.

Preview the settings of a Template

To preview the settings of a saved Template, select a saved Revoke permissions template, and then click View Details button. The settings will be displayed in a window as shown below:


Saved Permissions Template
Select any template from the list of saved templates to proceed. Click Open to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
Grant permissions task2
for the common share.
Grant
Grant permissions task1
for the Admin share folder
Grant
Revoke permissions task2
for the common share
Revoke
Revoke permissions task1
for Admin share
Revoke
View Details
Close
Summary
Report Name: Revoke permissions task1
Selected Revoke Mode:
Revoke the selected set of Accounts and their permissions from the selected shared folder(s)/file(s) permissions list.
Account Selection Mode:
Selected Accounts
Selected Security Principals:
1. vsspro\Alex
2. Vsspro\james
Close

Modify Permissions

How to view the share permissions?

How to grant permissions for a shared folder / file?

How to add new accounts to the folder / file permissions list?

How to replace an account with another account in the shared folder / file permissions list?

How to remove the selected account from shared folder / file permissions list?

How to allow inheritance from the parent to current folder / file permissions?

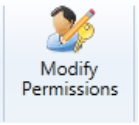
How to block inheritance from the parent to the current folder / file permissions?

How to modify the basic permissions for an account?

How to modify the advanced permissions for an account?

How to view the share permissions?

The **Modify Permissions** feature allows you to view and modify the entire file system permissions. You can use many options to modify the permissions of shares. With the option **Add** you can add an account with a permission "Read and Execute". With the option **Remove** you can remove an account and its explicit permissions from the share's permissions list. You can also edit the existing permissions and Allow and Block inheritance from the parent object.

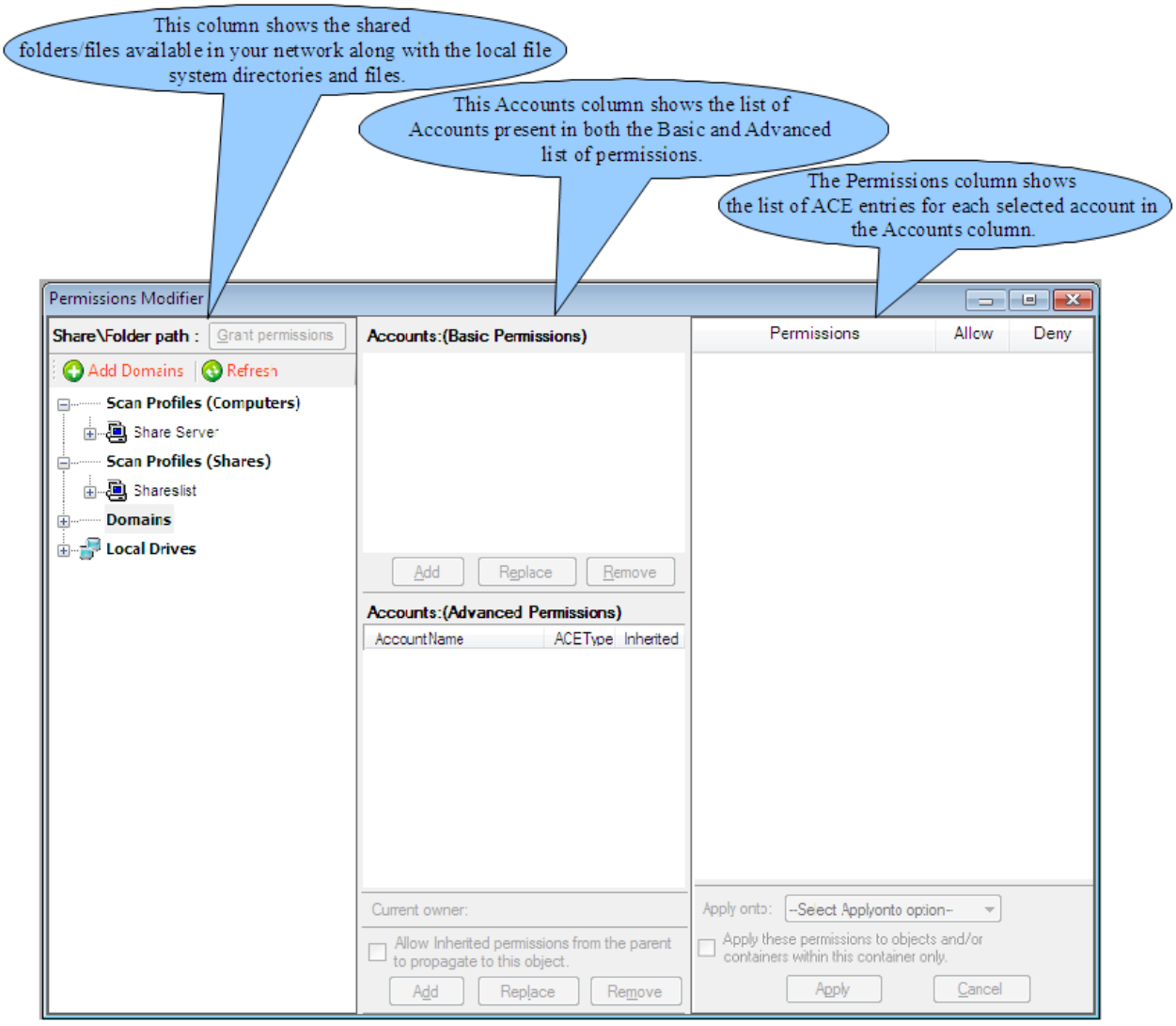
Click on 

button.

The Modify Permissions window will be displayed as shown below:

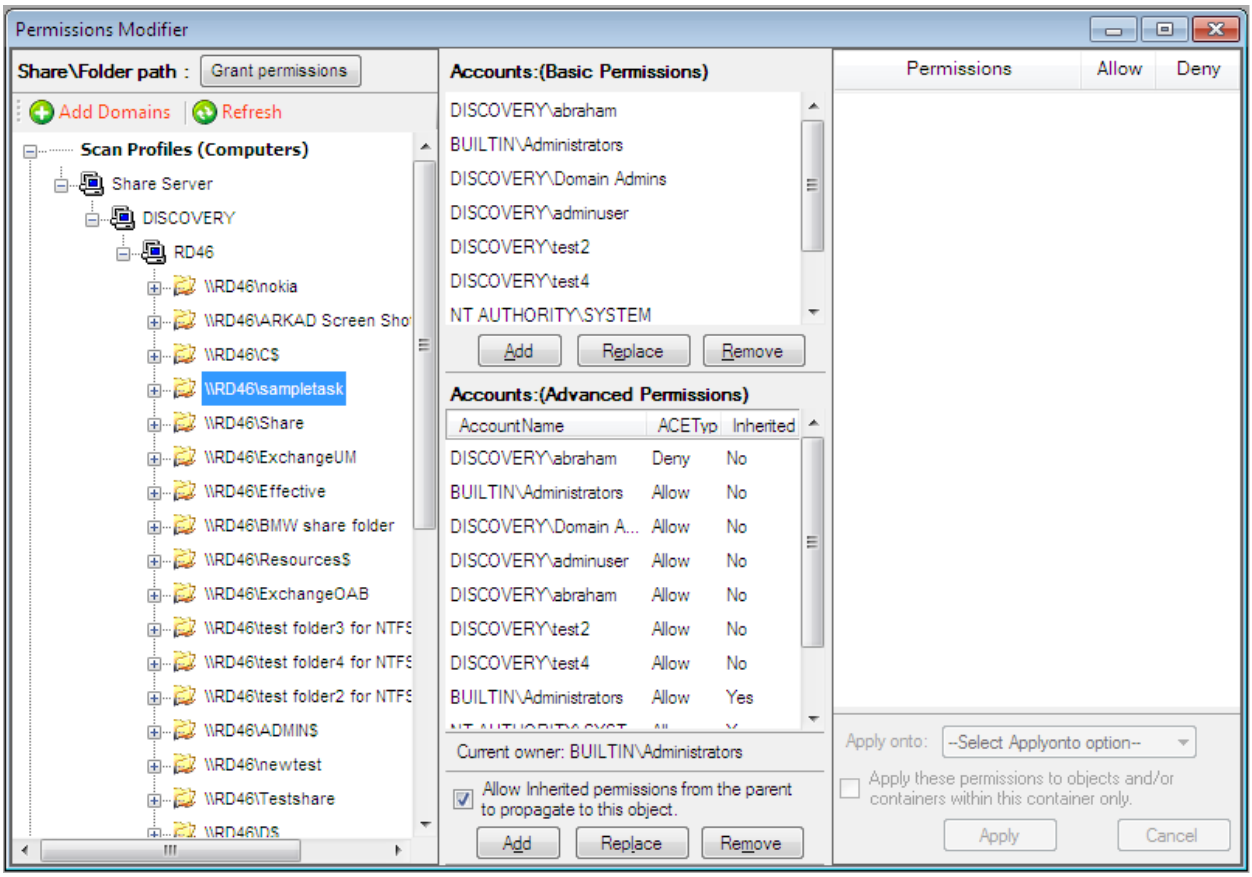
Step 1: Select folder/file path

Select folder/file path by using the option below.



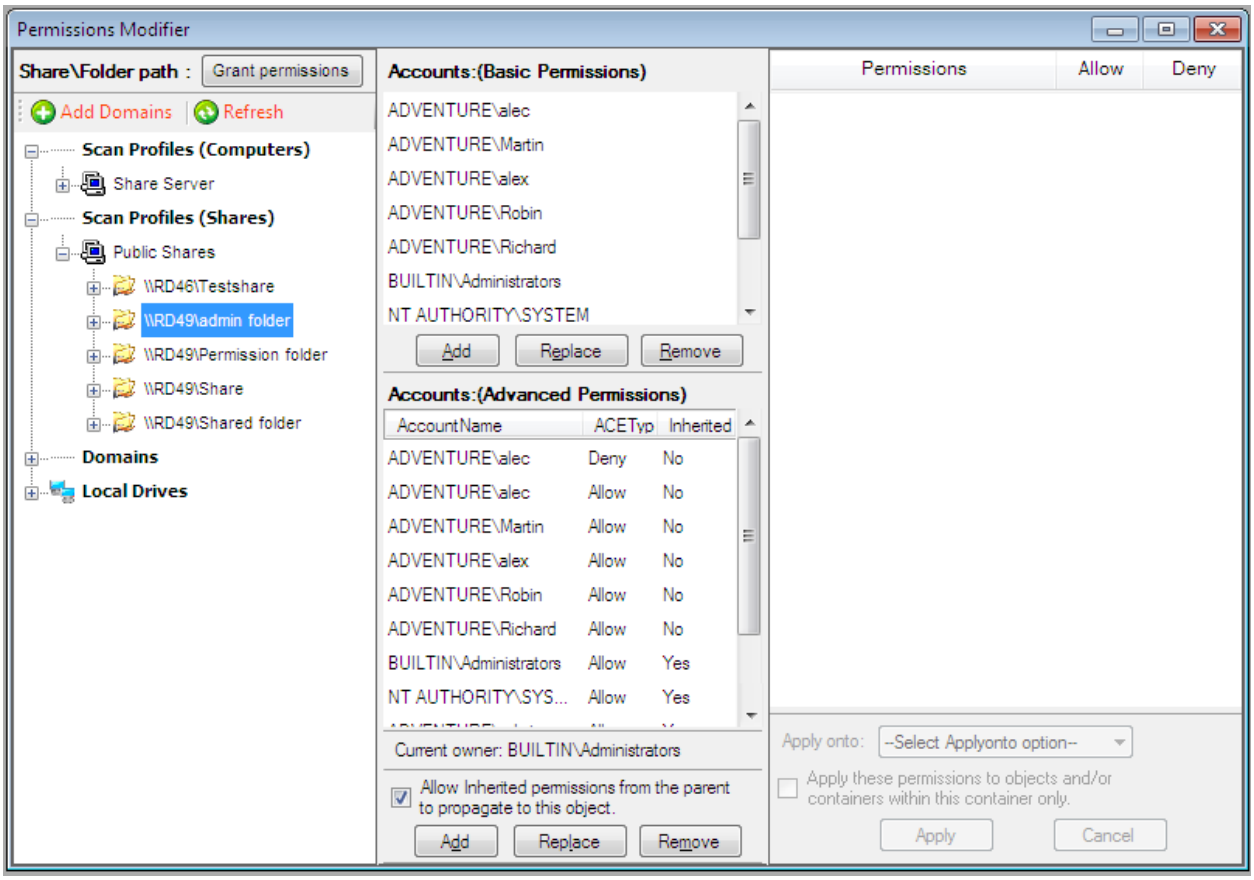
Select **Scan Profiles (Computers)** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file.
- Select a shared folder/file path.



Select **Scan Profiles (Shares)** and follow the steps below.

- Select Shares profile and enumerate its shared folder(s)/file(s) list.
- Select a shared folder/file path.

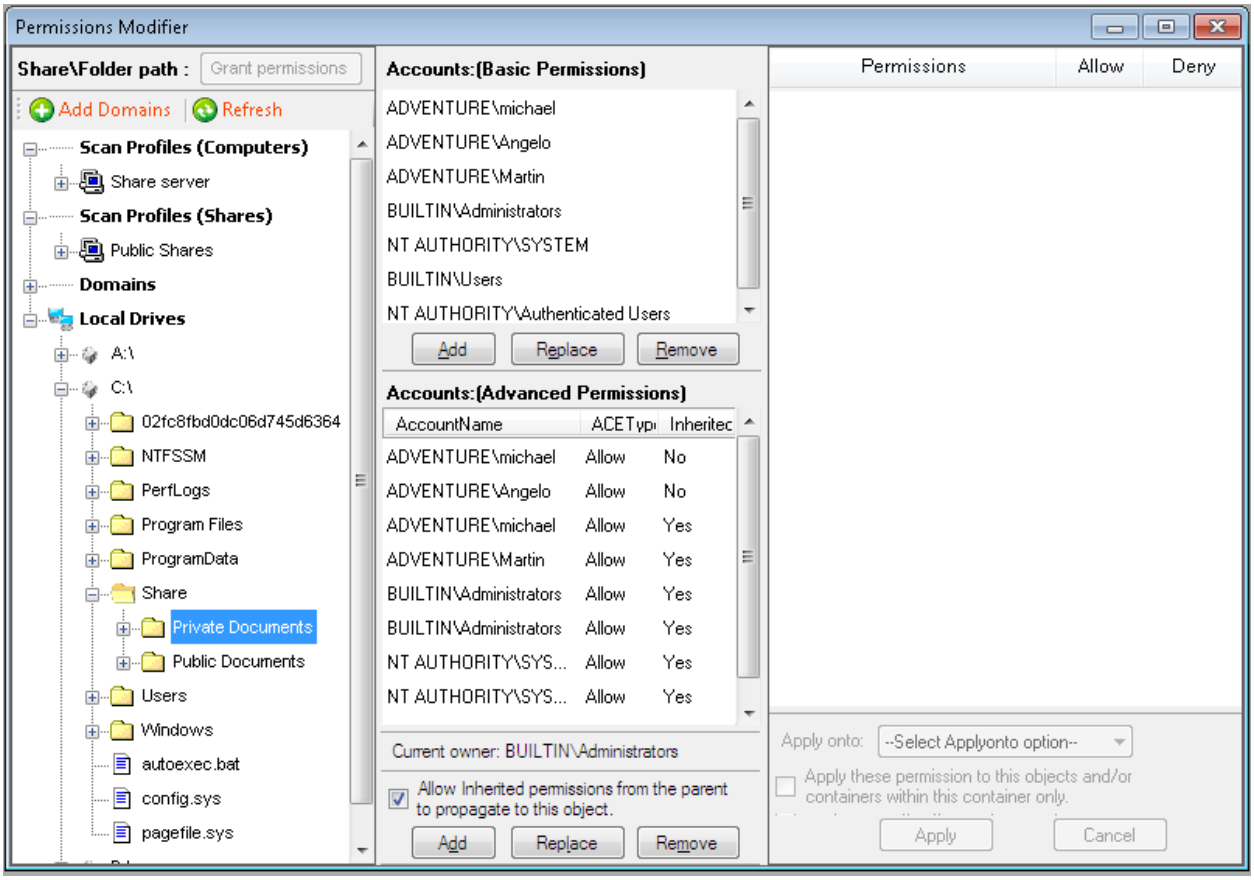


Select **Domains** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file path.
- Select a shared folder/file path.

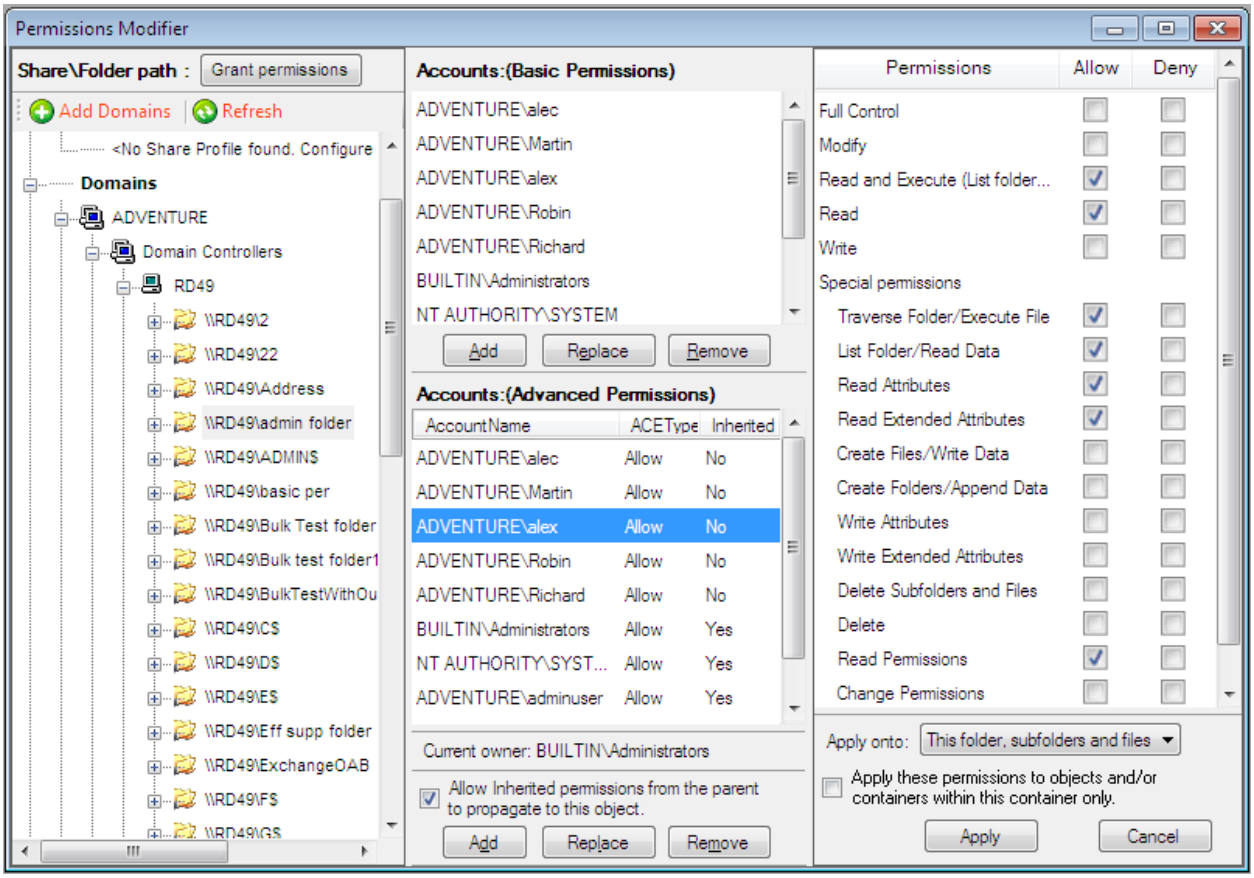
Select **Local Drives** and follow the steps below.

- Select and traverse one or more directory to enumerate its subfolders and files.
- Select a directory or subfolder/file path.



Step 2: Select an Account

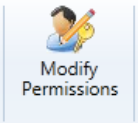
Select an account from the Basic or Advanced permissions list. After selecting an account, permissions of that account would be shown in the last column as shown below.



You may also verify the inheritance from the parent object (allowed or blocked) to this current object by using the option "Allow inherited permissions from the parent to propagate this object". If this option is checked then the inheritance from the parent to this current object has been allowed, otherwise if unchecked, it has been blocked.

How to Grant Permissions for selected Shares?

The **Grant Permissions** feature allows you to grant permissions to the Shares. You can use many options like Add the new permissions to the account's existing permissions, Replace the account's existing permissions with the new permissions, etc. You may select options to Allow, Block inheritance from the parent object and also Replace all child objects existing permissions with the inheritable permissions from this object while granting permissions for accounts.

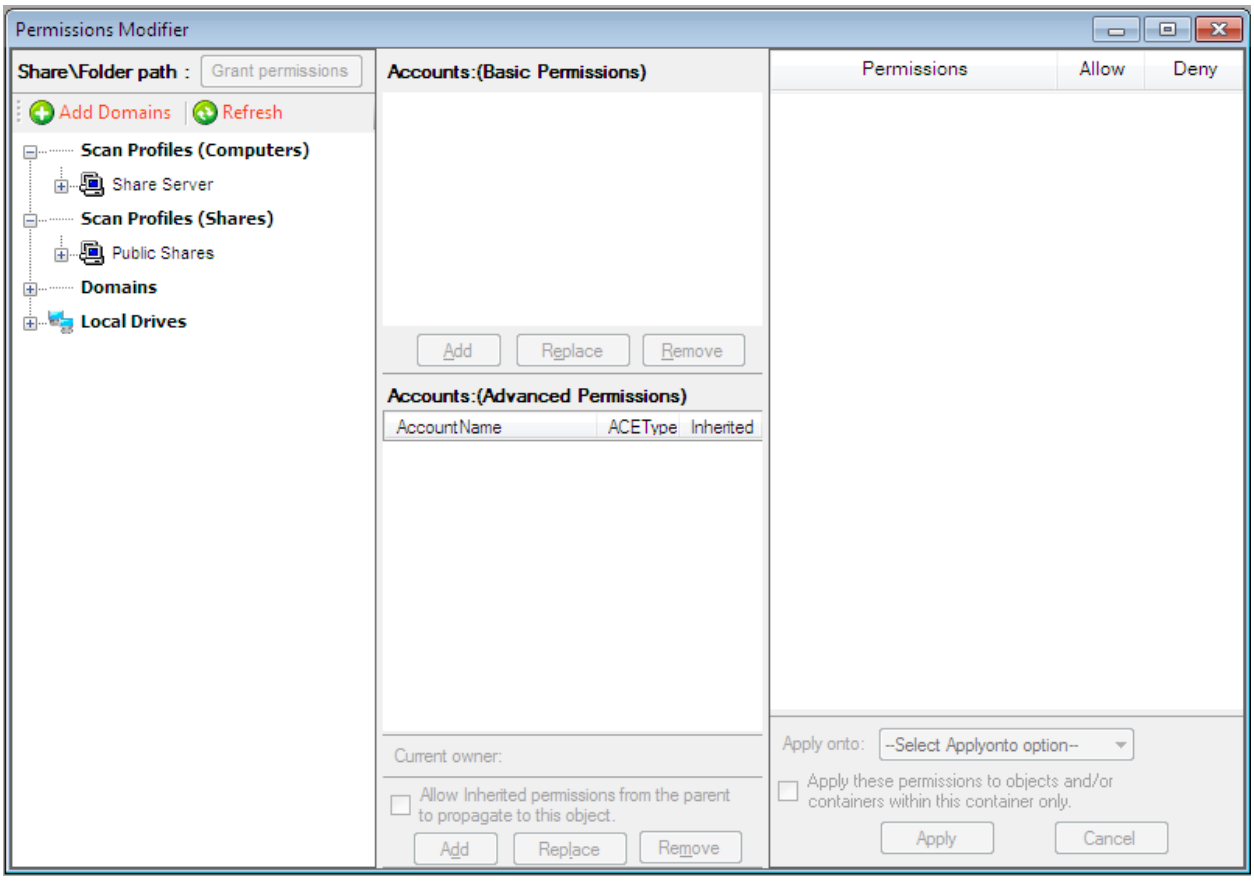
Click on 

button.

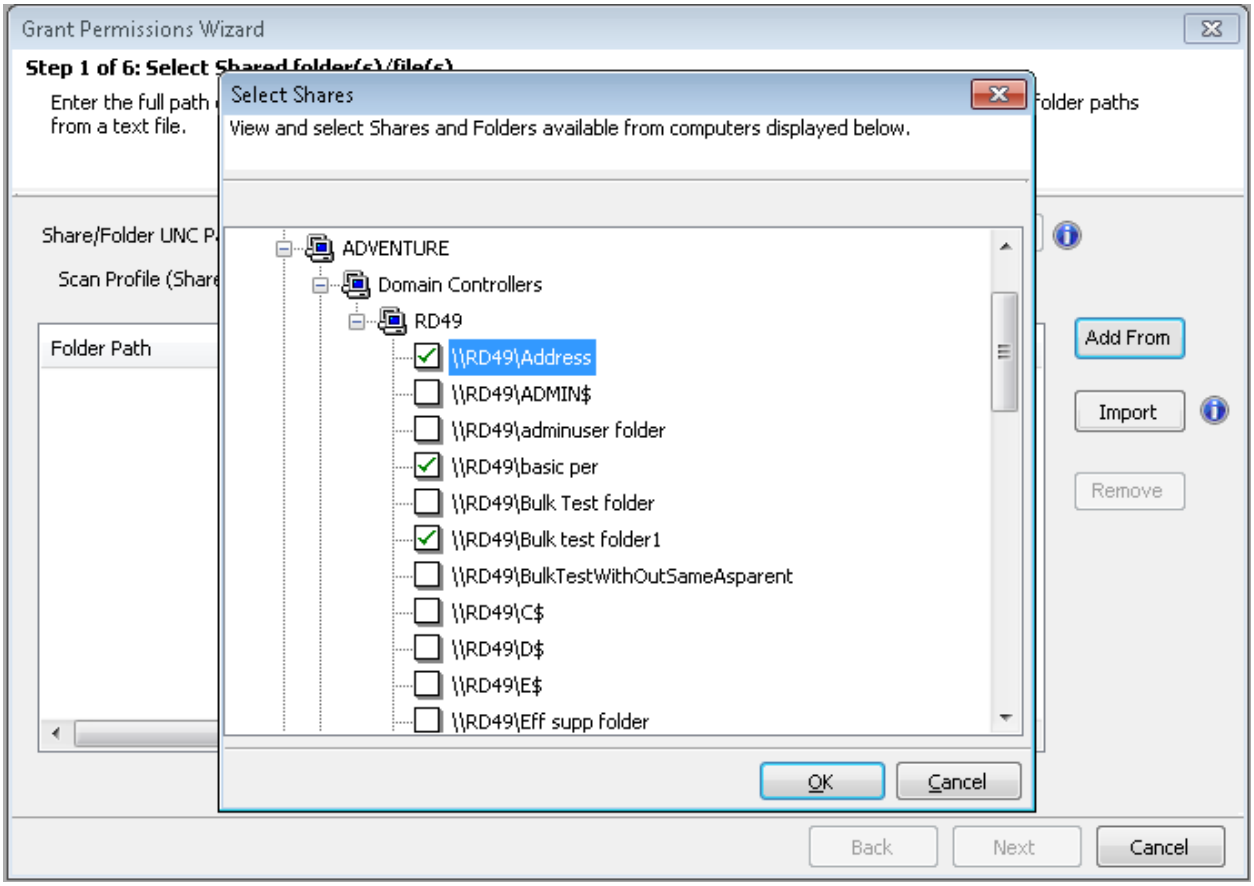
The Grant Permissions window will be displayed as shown below:

Step 1: Select shared folder(s)/file(s)

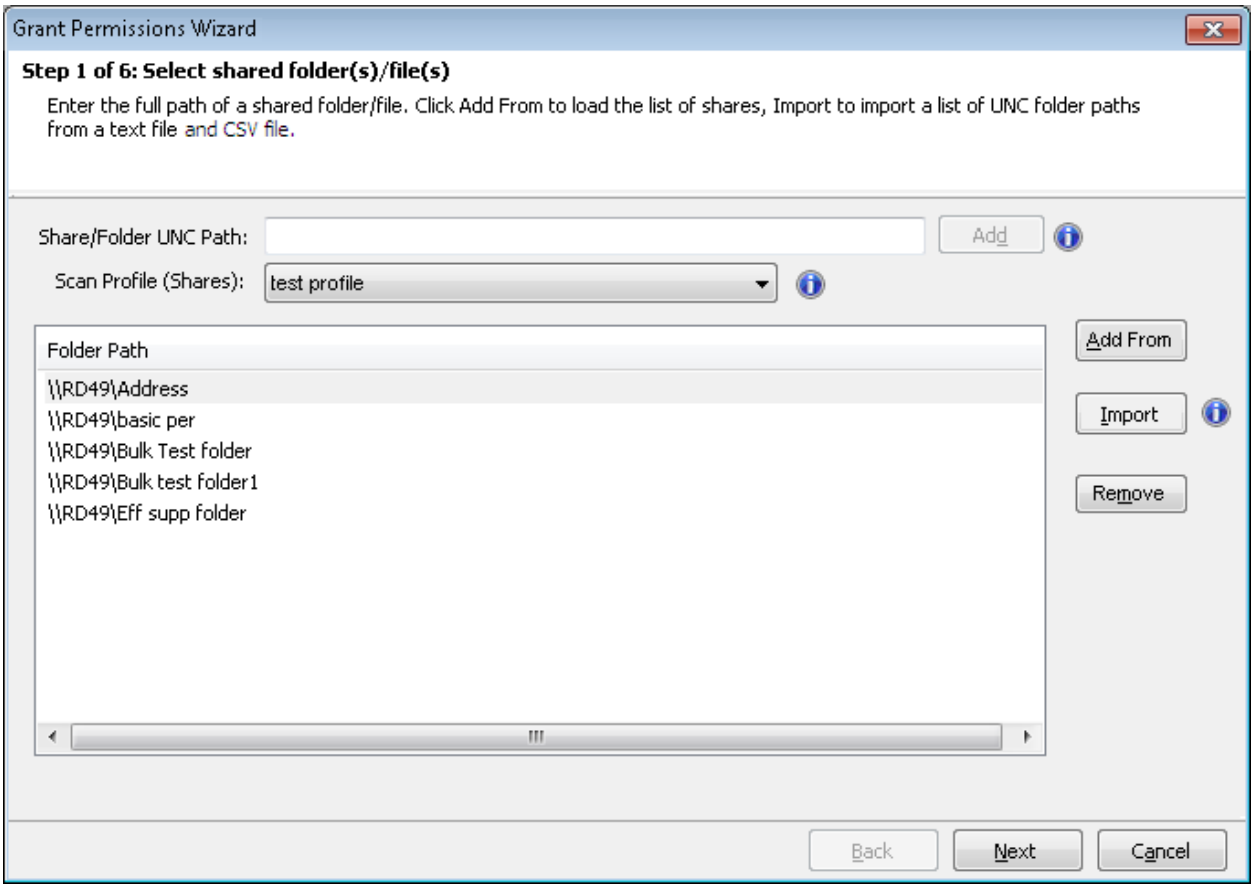
Select shared folder(s)/files by using any of the input options displayed



- Click the option **Add From**
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use **Select a Scan Profile (Shares)** option to use the shares added in the profile.

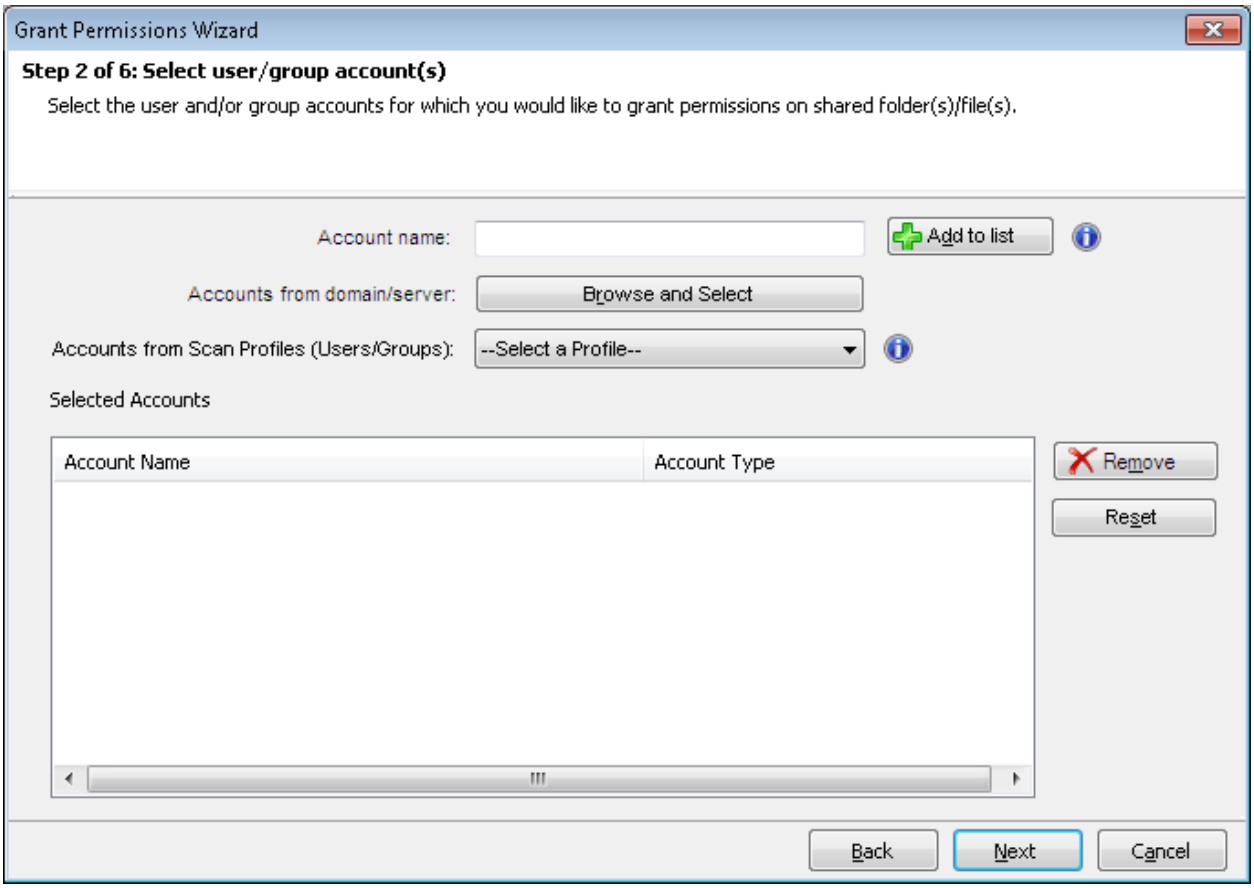


You may also type the UNC path of a shared folder that is not in the list and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared folder list from a text file by using the **Import** button.

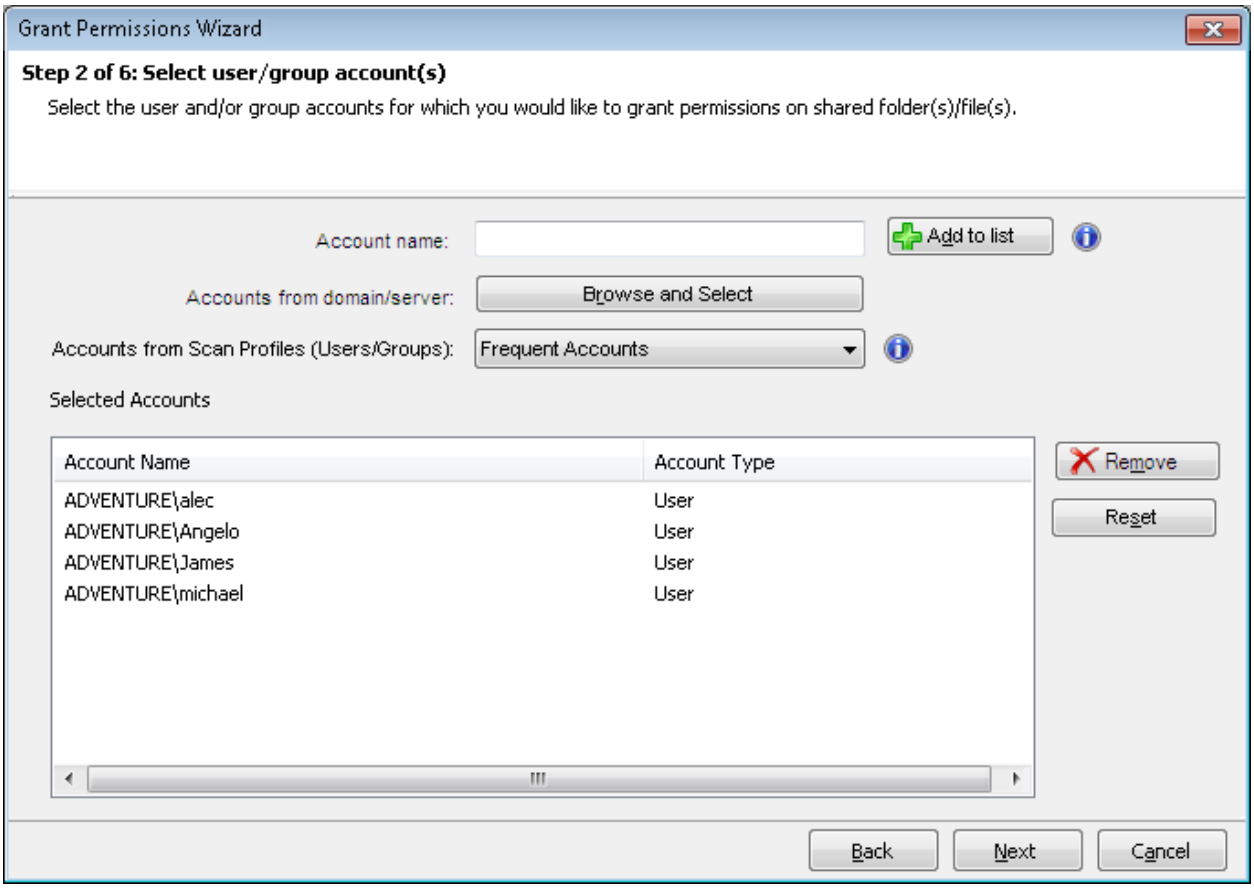
Click **Next** to proceed to the next step.

Step 2: Account Selection

1. Select the accounts, for which you wish to grant permissions.
2. The selected accounts will be added to the wizard as shown below:



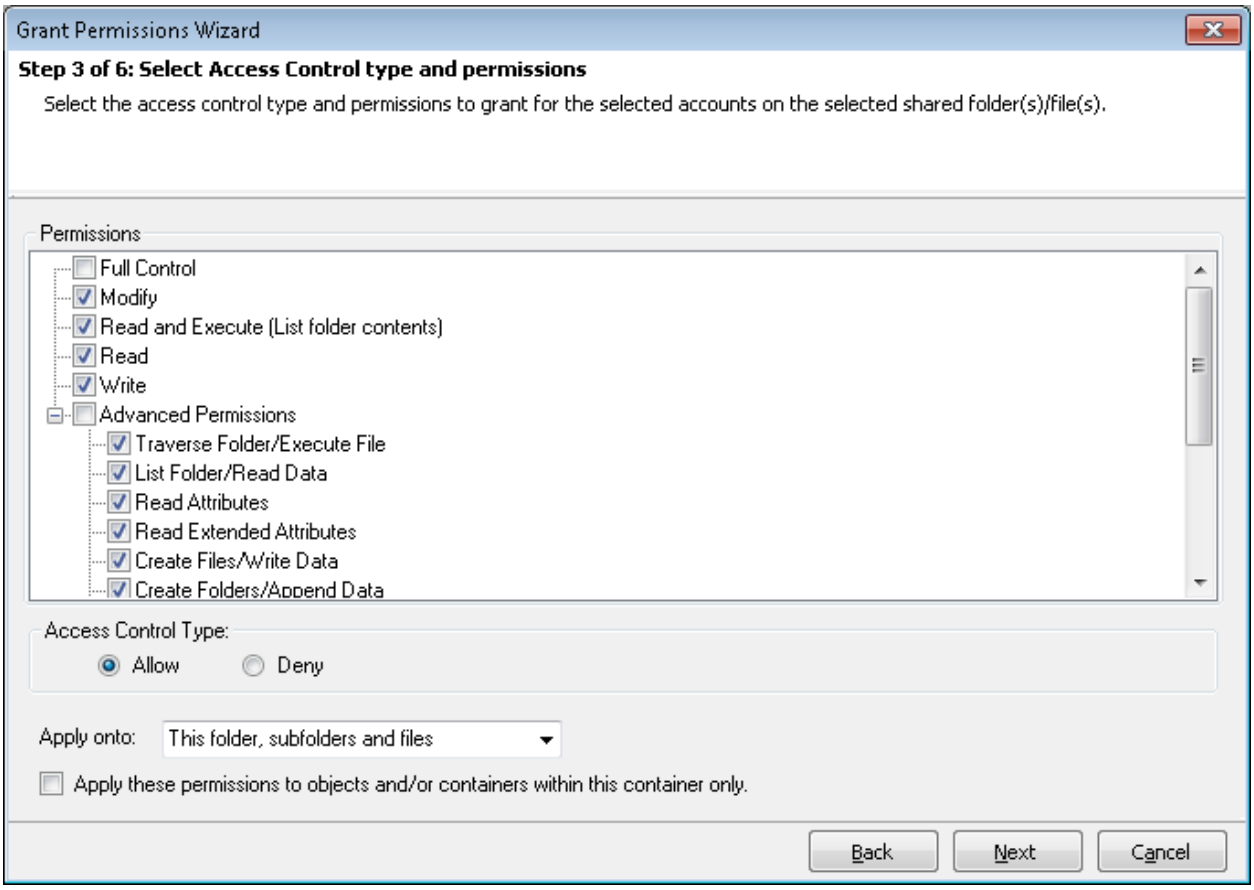
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile.



Click **Next** to proceed to the Next step.

Step 3: Select Access Control type and permissions

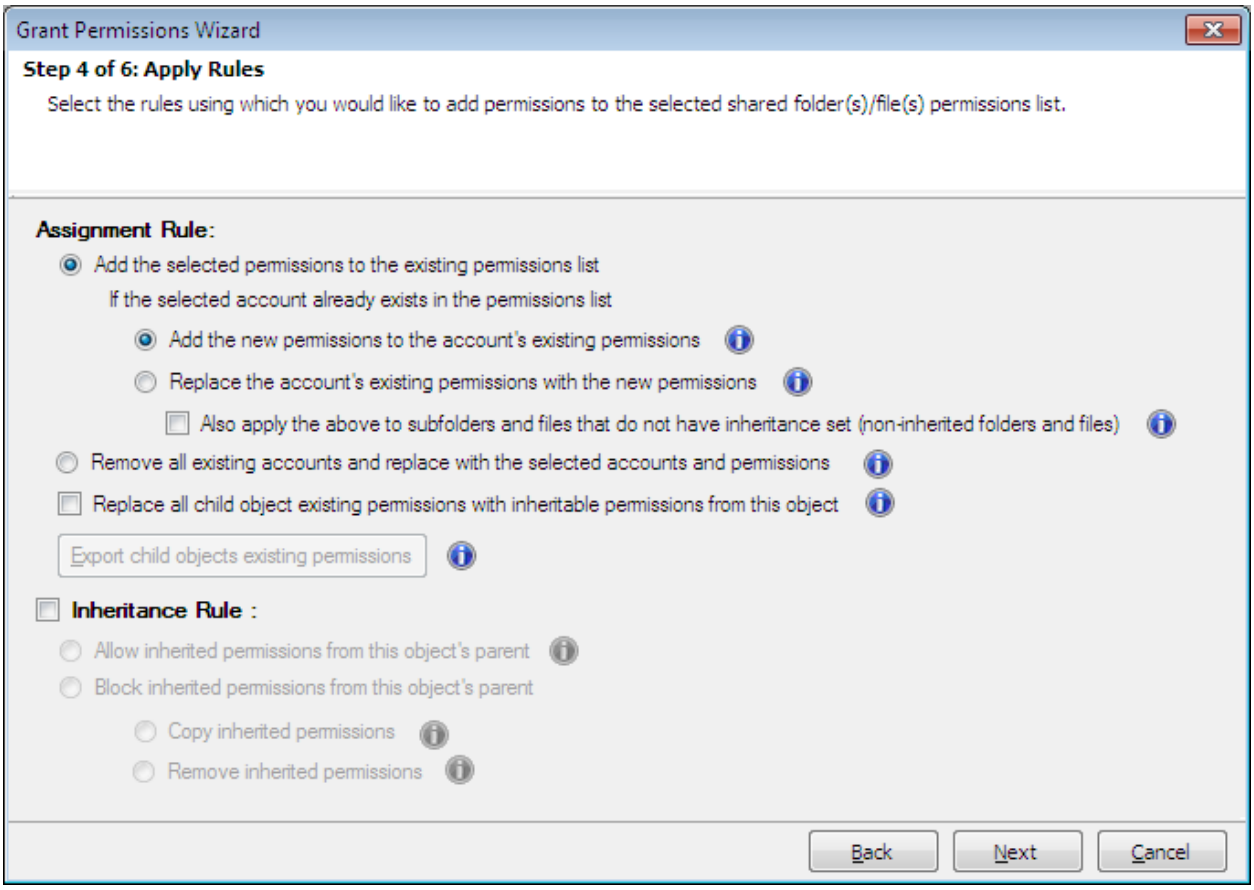
Select ACE type and permissions to grant for the selected accounts on the selected shared folder(s) /files(s)



Click **Next** to proceed to the next step.

Step 4: Apply the required rules to be used while assigning permissions

Select which rules to apply while assigning permissions.


Grant Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to add permissions to the selected shared folder(s)/file(s) permissions list.
Assignment Rule:
Add the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permissions from this object
Export child objects existing permissions
Inheritance Rule :
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

Add the new permissions to the account's existing permissions option will add the selected permissions to the existing permissions list and also it will not affect the existing permissions.

You may also use the below options to grant permissions and also apply inheritance by Inheritance rule

- Remove all existing accounts and replace with the selected accounts and permissions.
- Replace the account's existing permissions with the new permissions.
- Replace all child objects existing permissions with the inheritable permissions from this object.

Inheritance Rule:

- Allow inherited permissions from this object's parent.
- Copy inherited permissions.
- Remove inherited permissions.

Remove all existing accounts and replace with the selected accounts and permissions

This option will remove all existing accounts that have explicitly assigned permissions for the selected shared folder(s)/file(s) and replace them with the selected accounts and permissions. Note that this will not remove inherited permissions from parent folder.

Caution: All existing account permissions will be cleaned up completely and the newly selected permissions will be applied.

Example: If the share has 7 accounts then this option will remove all the 7 accounts and replace with the new selected accounts and permissions.

Replace the account's existing permissions with the new permissions

If a selected account already exists in the current list of permissions of the selected shared folder(s)/file(s), this option will replace all explicitly assigned account permissions with the newly selected permissions for that account.

Example: If the share already has some accounts with permissions like Allow Read and Write and if the same existing accounts selected with permissions Deny Modify to grant permissions then this option will replace the existing accounts previous permissions (Allow Read and Write) with new permission (Deny Modify). Otherwise if the selected account not exist in the share permissions list then it will add into the permissions list.

Replace all child objects existing permissions with the inheritable permissions from this object

This option will remove explicitly defined permissions on all descendants of the selected shared folder(s)/file(s) and replace them with inheritable permissions from the selected shared folder(s)/file(s).

Example: If the share has some subfolders with the explicitly assigned permissions and some subfolders with blocked inheritance then this option will remove all explicitly assigned permissions of subfolders and allow inherited permissions from the parent object.

Allow inherited permissions from this object's Parent

This option will allow the selected shared folder(s)/file(s) to inherit permissions from its parent object.

Example: If the share do not have any inherited permissions and the inheritance from the parent object blocked then this option will allow inherited permissions from the parent object.

Copy inherited permissions

This option will copy the permission entries that were previously inherited from the parent to this selected shared folder(s)/file(s).

Example: If the share already allowed to inherit permissions from parent object then this option will remove the inheritance and add the inherited permissions as explicit permissions in the permissions list.

Remove inherited permissions

This option will remove the permission entries that were previously inherited from the parent and keep only those permissions explicitly defined/granted here.

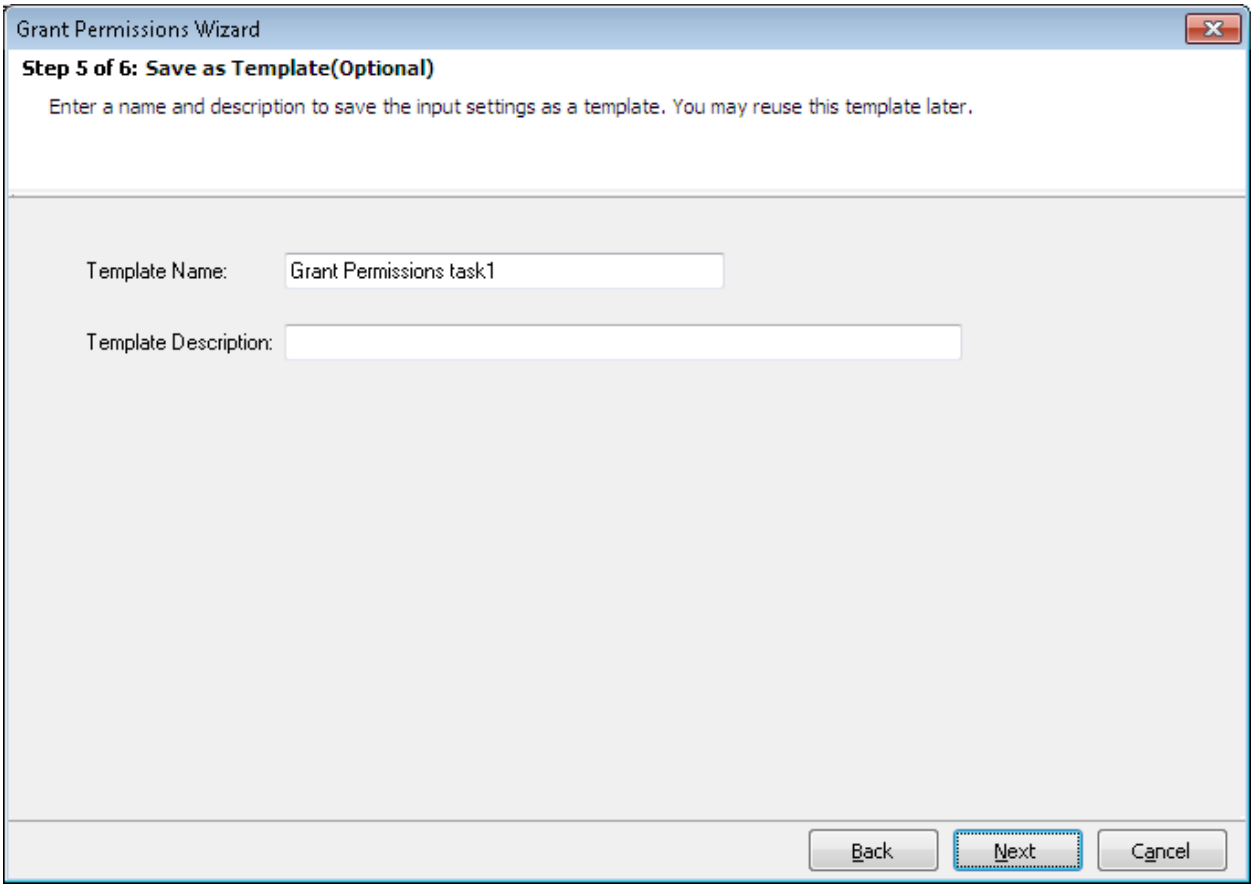
Caution: Removing permission inheritance from parent may break permissions/policies designed with the default inheritance option enabled. Use this option after a careful review.

Example: If the share is already set to inherit permissions from parent object then this option will remove the inheritance from parent object.

Click Next to proceed to the Next step

Step 5: Save as template

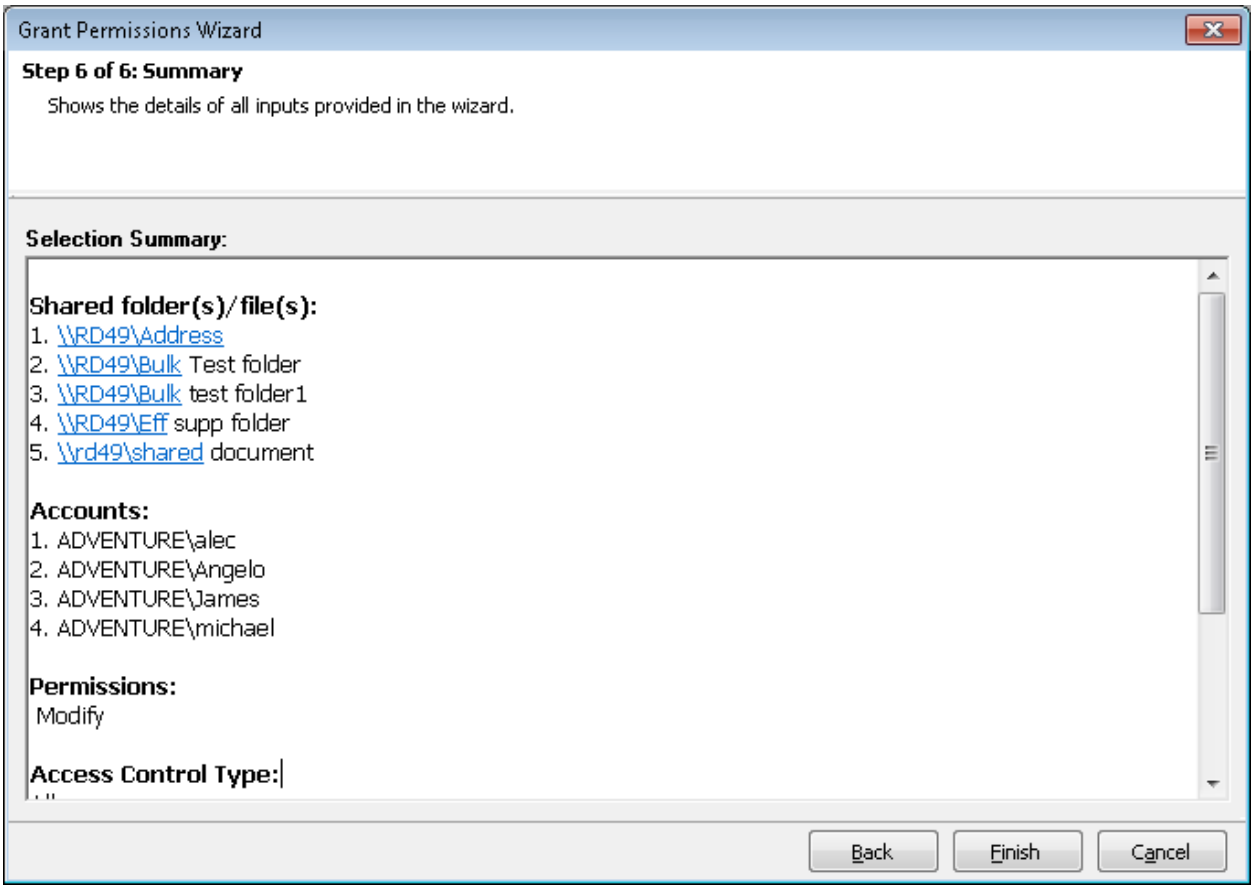
Enter a name and description to save these settings as a template for reuse later.


Grant Permissions Wizard
Step 5 of 6: Save as Template(Optional)
Enter a name and description to save the input settings as a template. You may reuse this template later.
Template Name:
Grant Permissions task1
Template Description:
Back
Next
Cancel

Click **Next** to proceed to the next step

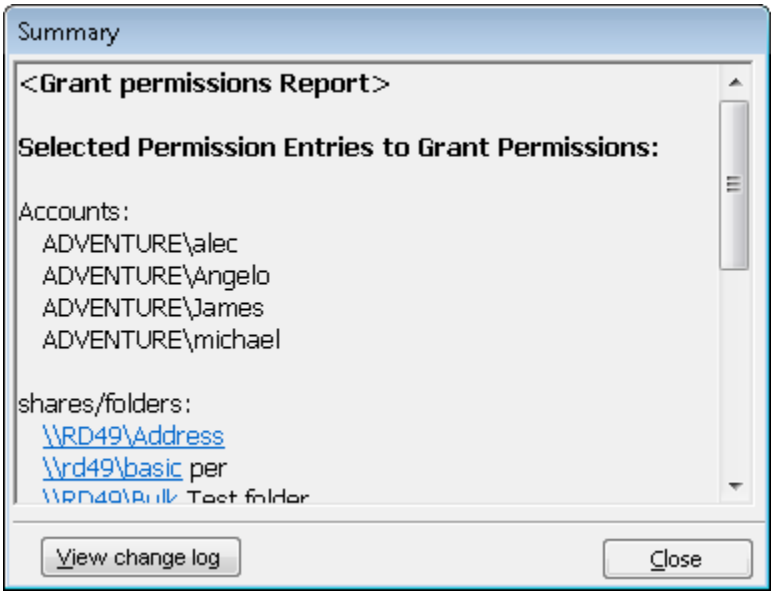
Step 6: Summary

This step displays the summary of all the input data along with the selected options.



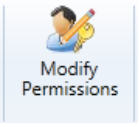
Click **Finish** to complete the Grant Permissions wizard.

Permissions will be granted as specified in the wizard. The summary of all the input data would be shown below along with the option "View change log" to view the task completion status.



How to add new accounts to the folder/file permissions list?

The **Modify Permissions** feature allows you to add new accounts with the permission **ReadandExecute** to the permissions list.

Click on 

button.

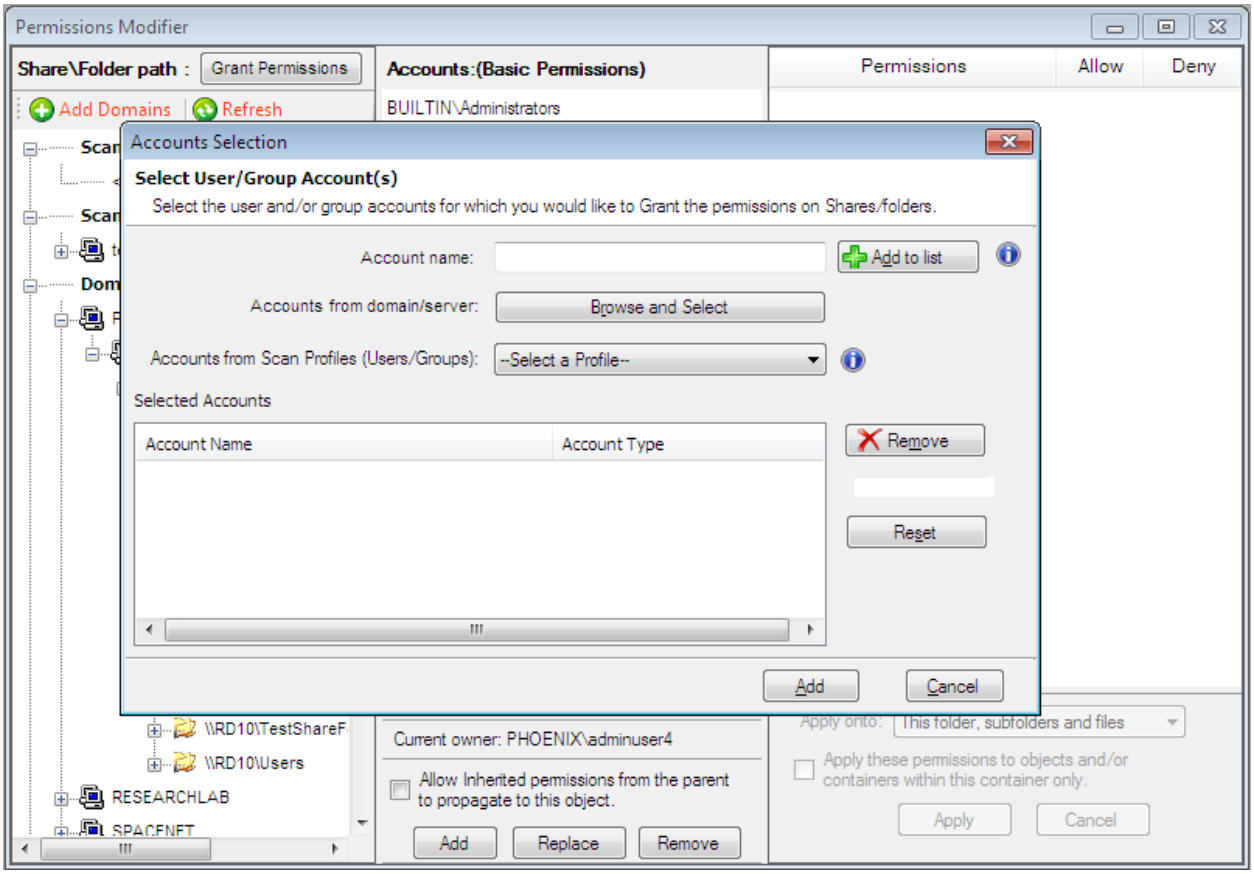
The Modify Permissions window will be displayed.

Step 1: Select folder/file path

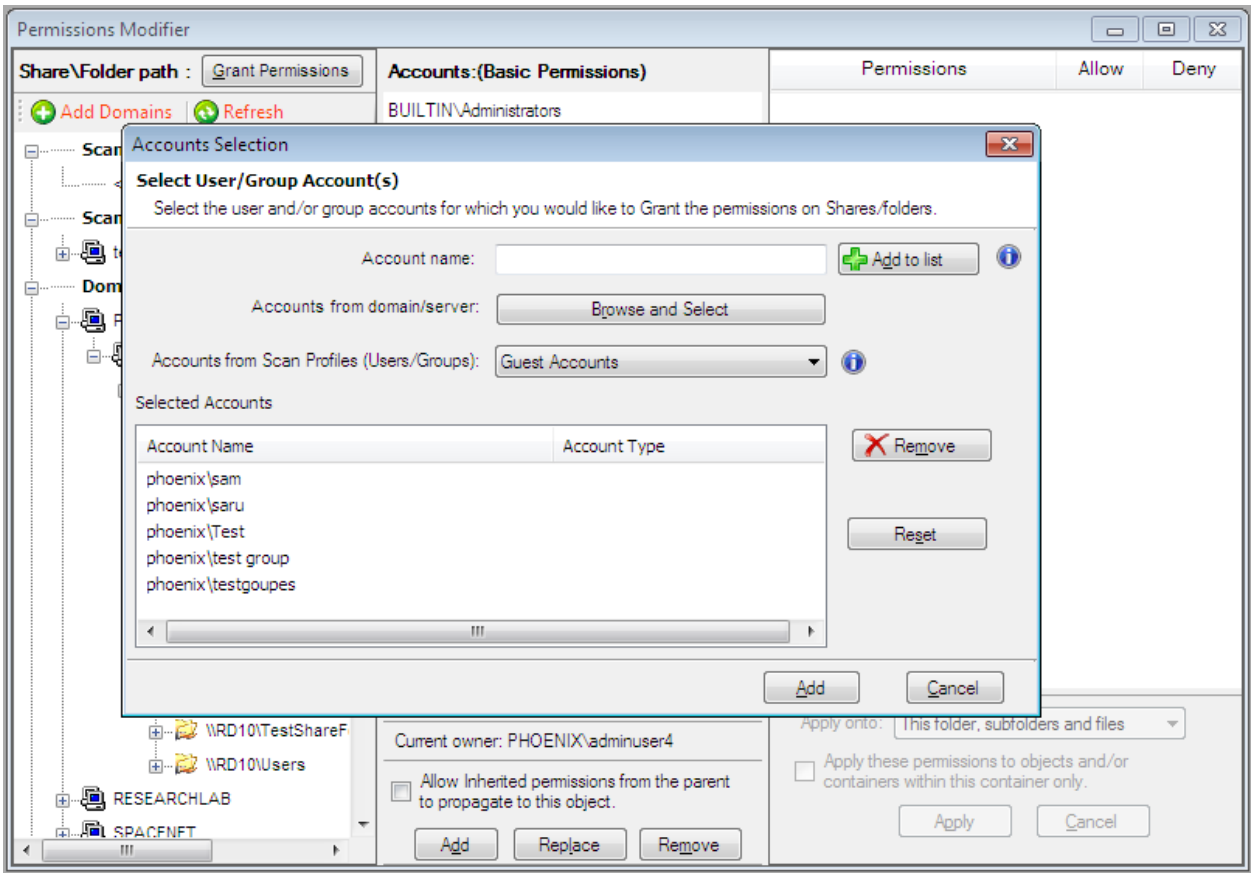
- Follow the list of options to enumerate the shared folder/file as outlined in How to enumerate shared folders/files?

Step 2: Click Add button and select accounts

Click **Add** button in the Basic or Advanced permissions. The Account Selection window will be displayed as shown below.



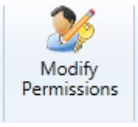
1. Select the user or group, for which you wish to add into the folder/file permissions list.
2. The selected accounts will be added to the wizard as shown below:



- Click **Add** button in the Accounts selection window.
- The newly added accounts will be displayed as shown below.

How to enumerate shared folders/files?

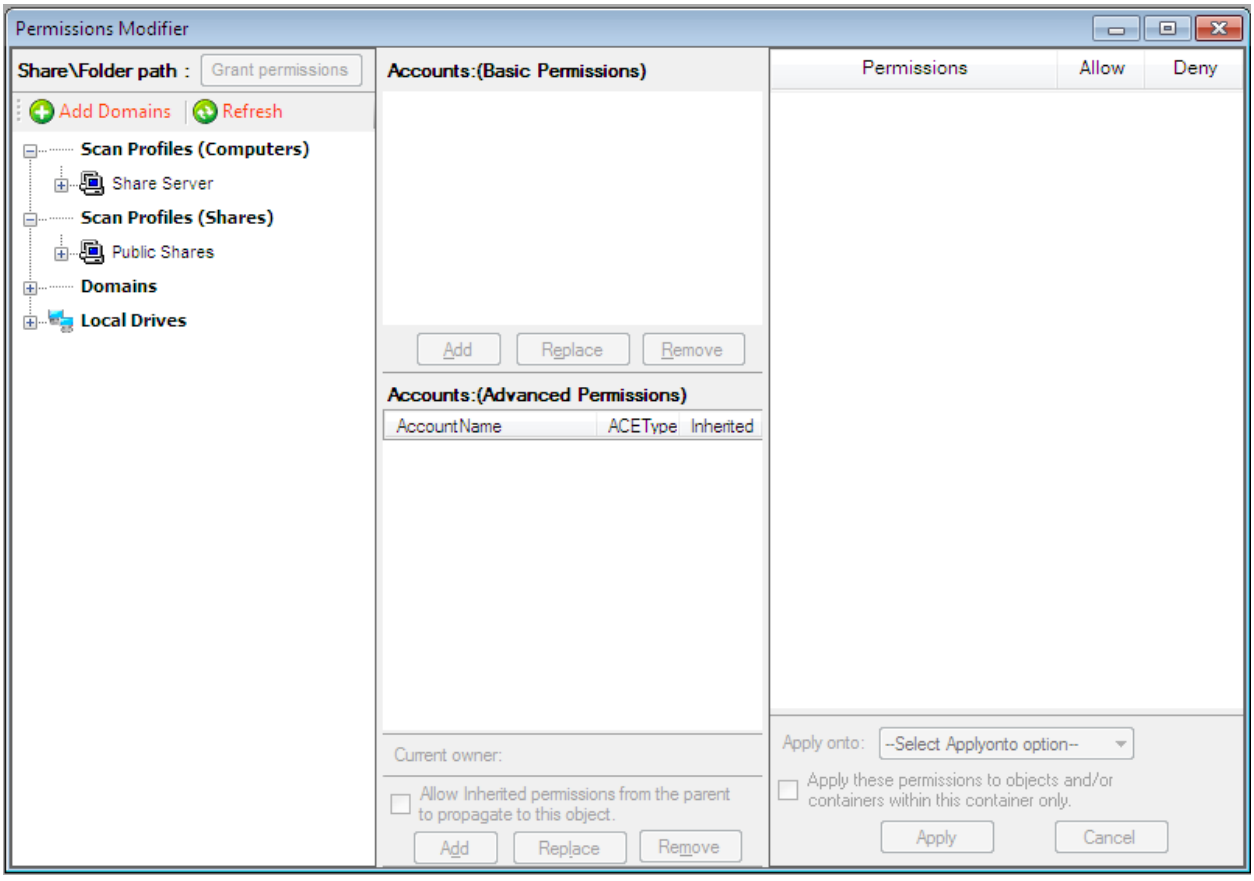
The **Modify Permissions** feature allows many options to enumerate the shared folders/files in the entire network. You can also enumerate and view the folders and files in the local file system.

Click on 

button.

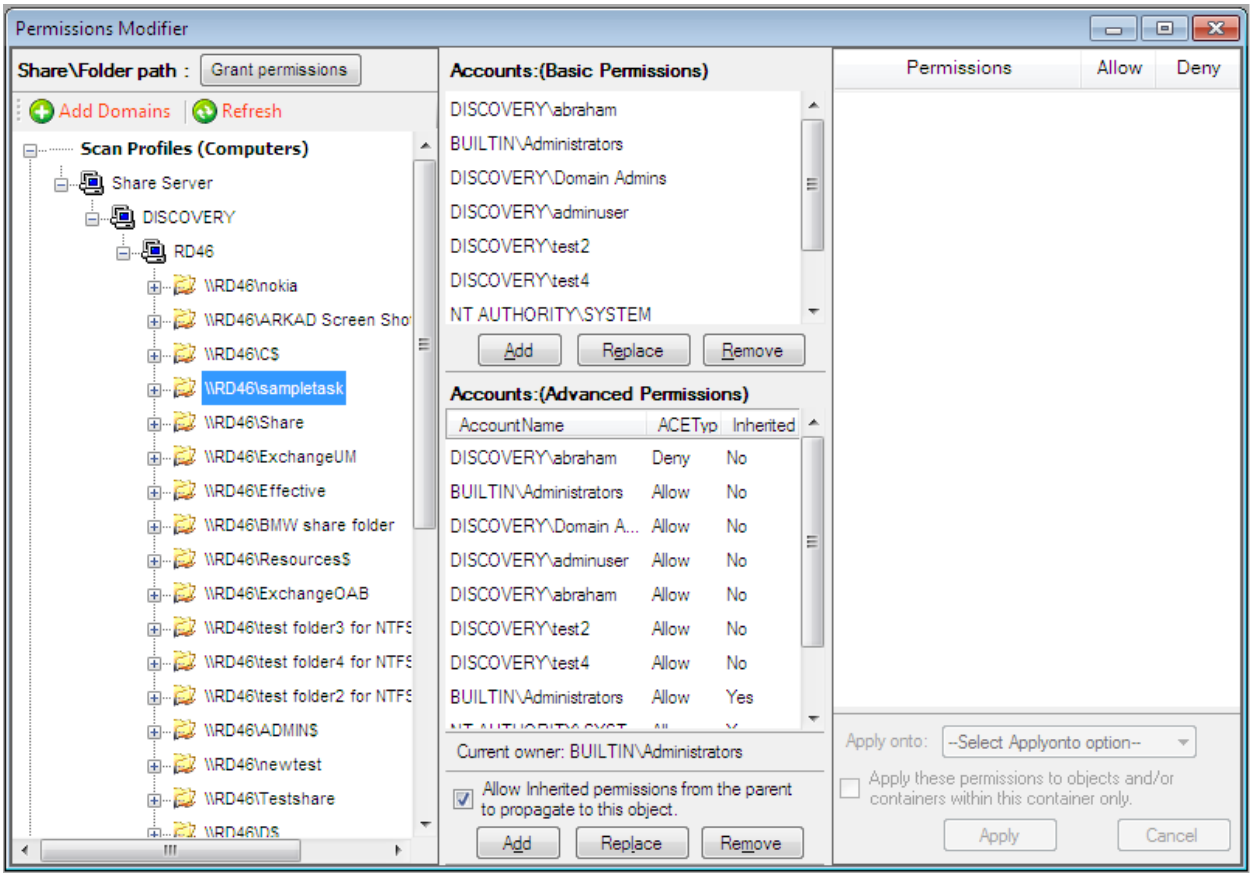
The Modify Permissions window will be displayed as shown below. Here is the list of ways you can enumerate the shared folders/files in the network.

- Scan Profiles(Computers)
- Scan Profiles(Shares)
- Domains
- Local Drives



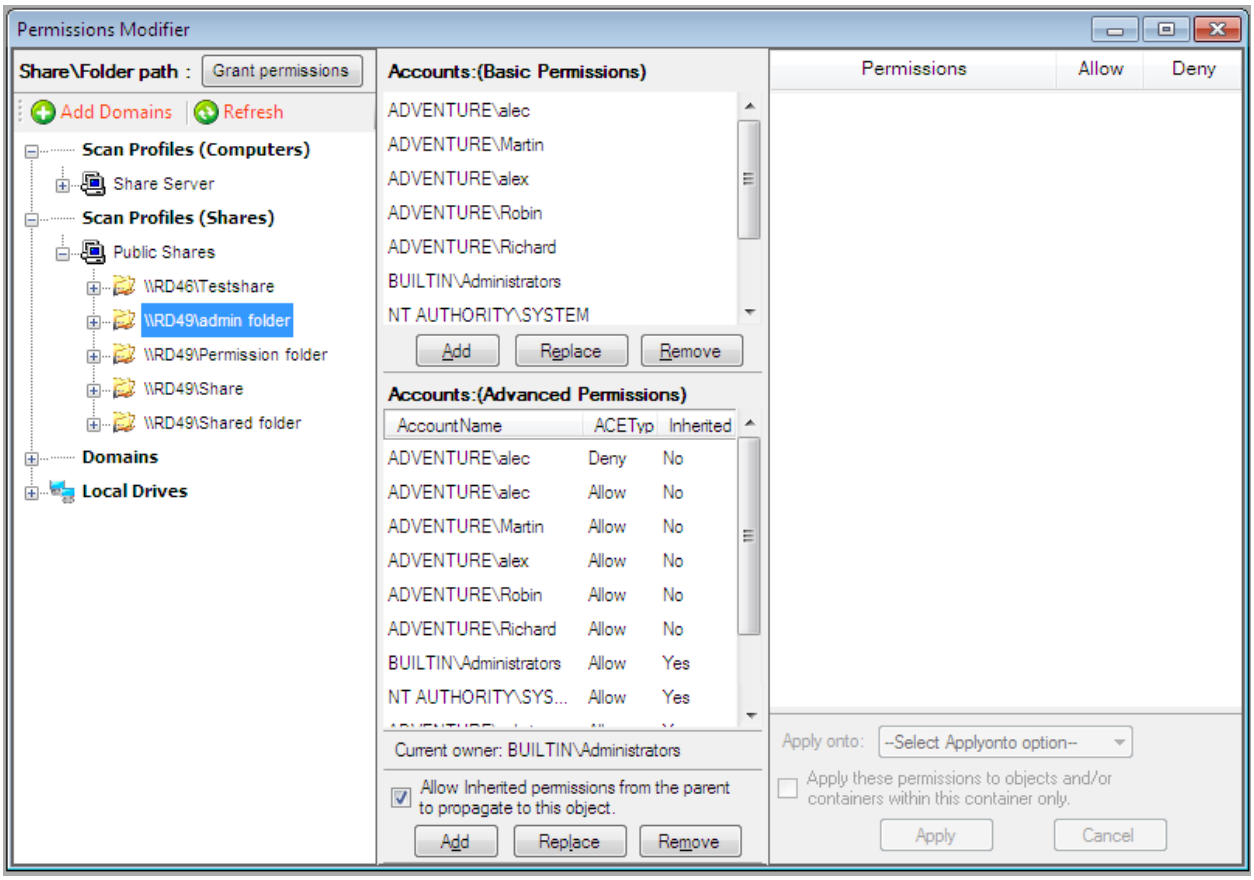
Select **Scan Profiles (Computers)** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file.
- Select a shared folder/file path.



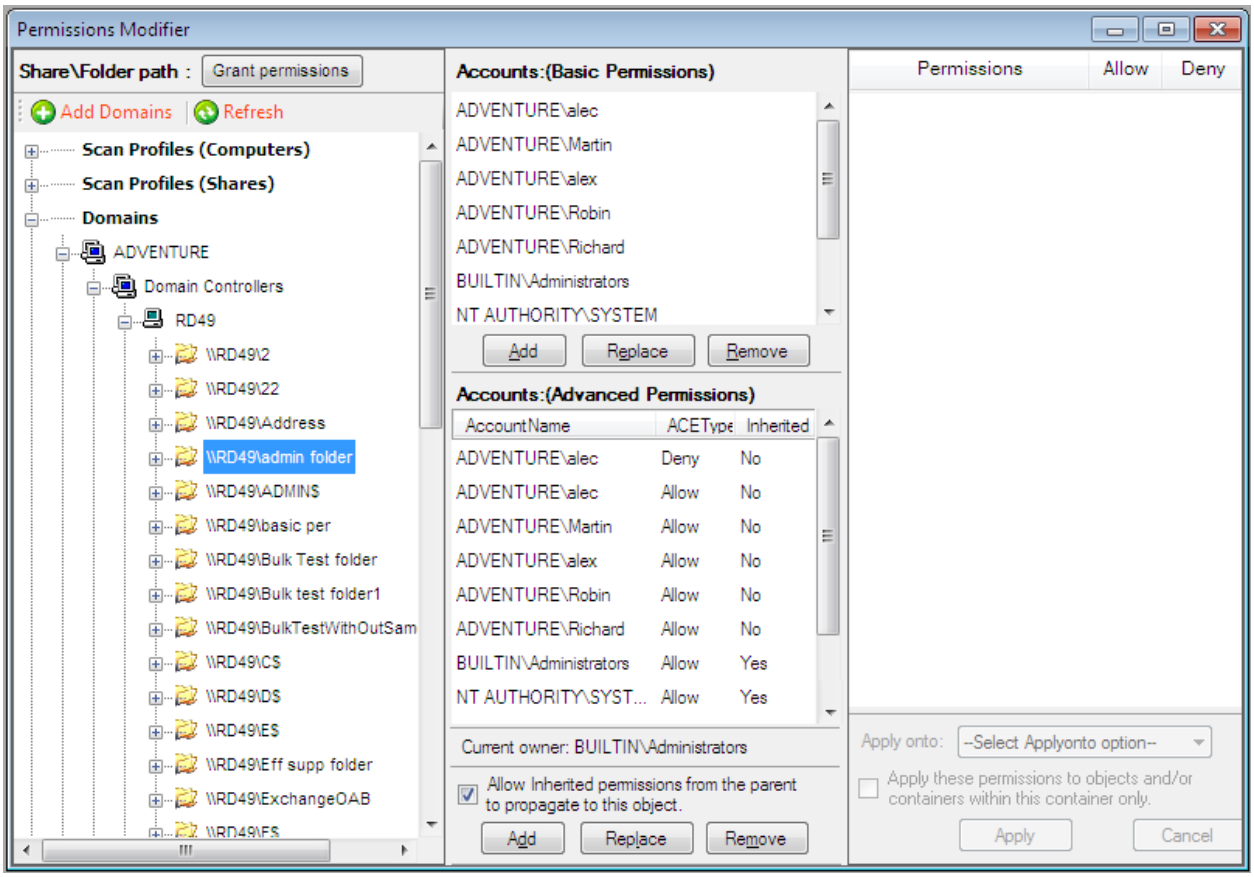
Select **Scan Profiles (Shares)** and follow the steps below.

- Select shares profile and enumerate its shared folder(s)/file(s) list.
- Select a shared folder/file path.



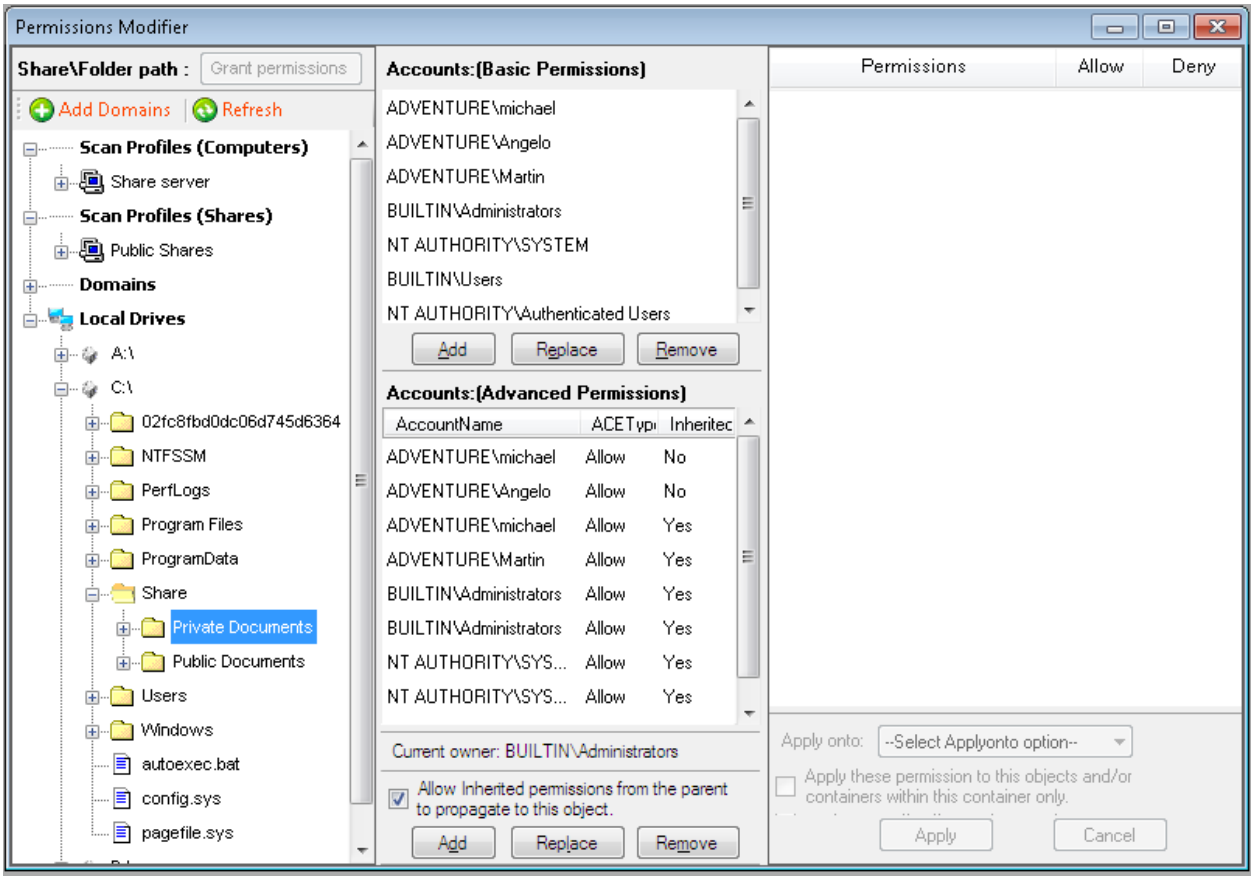
Select **Domains** and follow the steps below.

- Select one or more servers to enumerate its shared folder/file path.
- Select a shared folder/file path.



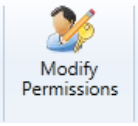
Select **Local Drives** and follow the steps below.

- Select and traverse one or more directory to enumerate its subfolders and files.
- Select a directory or subfolder/file path.


Permissions Modifier
Share\Folder path :
Grant permissions
Add Domains
Refresh
Scan Profiles (Computers)
Share server
Scan Profiles (Shares)
Public Shares
Domains
Local Drives
A:\
C:\
02fc8fbd0dc06d745d6364
NTFSSM
PerfLogs
Program Files
ProgramData
Share
Private Documents
Public Documents
Users
Windows
autoexec.bat
config.sys
pagefile.sys
Accounts:(Basic Permissions)
ADVENTURE\michael
ADVENTURE\Angelo
ADVENTURE\Martin
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
BUILTIN\Users
NT AUTHORITY\Authenticated Users
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACETyp
Inheritec
ADVENTURE\michael Allow No
ADVENTURE\Angelo Allow No
ADVENTURE\michael Allow Yes
ADVENTURE\Martin Allow Yes
BUILTIN\Administrators Allow Yes
BUILTIN\Administrators Allow Yes
NT AUTHORITY\SYS... Allow Yes
NT AUTHORITY\SYS... Allow Yes
Current owner: BUILTIN\Administrators
Allow Inherited permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Apply onto:
--Select Applyonto option--
Apply these permission to this objects and/or containers within this container only.
Apply
Cancel

How to replace an account with another account in the shared folder/file permissions list?

The **Modify Permissions** feature allows you to replace an existing account with single or multiple accounts by retaining the same permissions in the permissions list. You can replace accounts on specified levels of sub-folder and also replace accounts on sub-folders that match the specified search pattern.

Click on 

button.

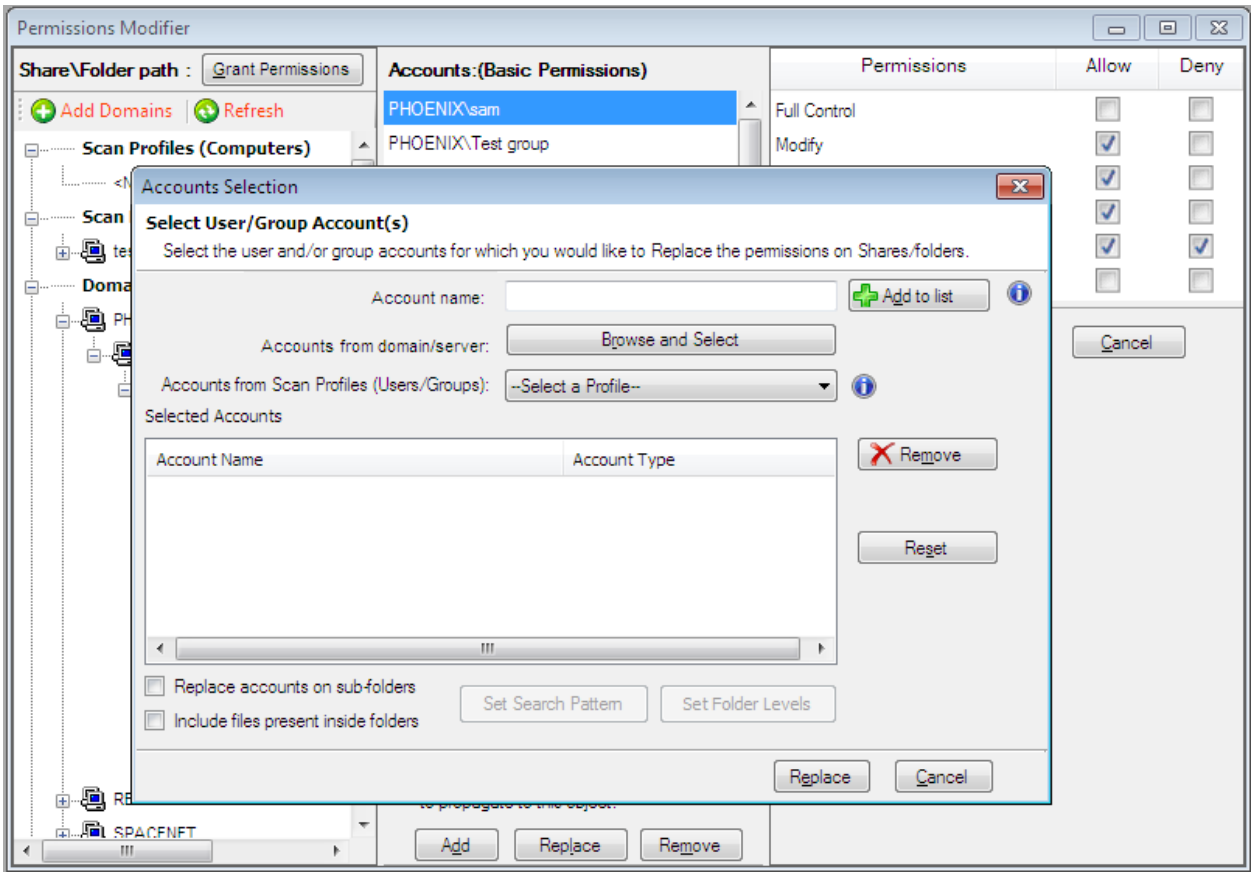
The Modify Permissions window will be displayed.

Step 1: Select folder/file path

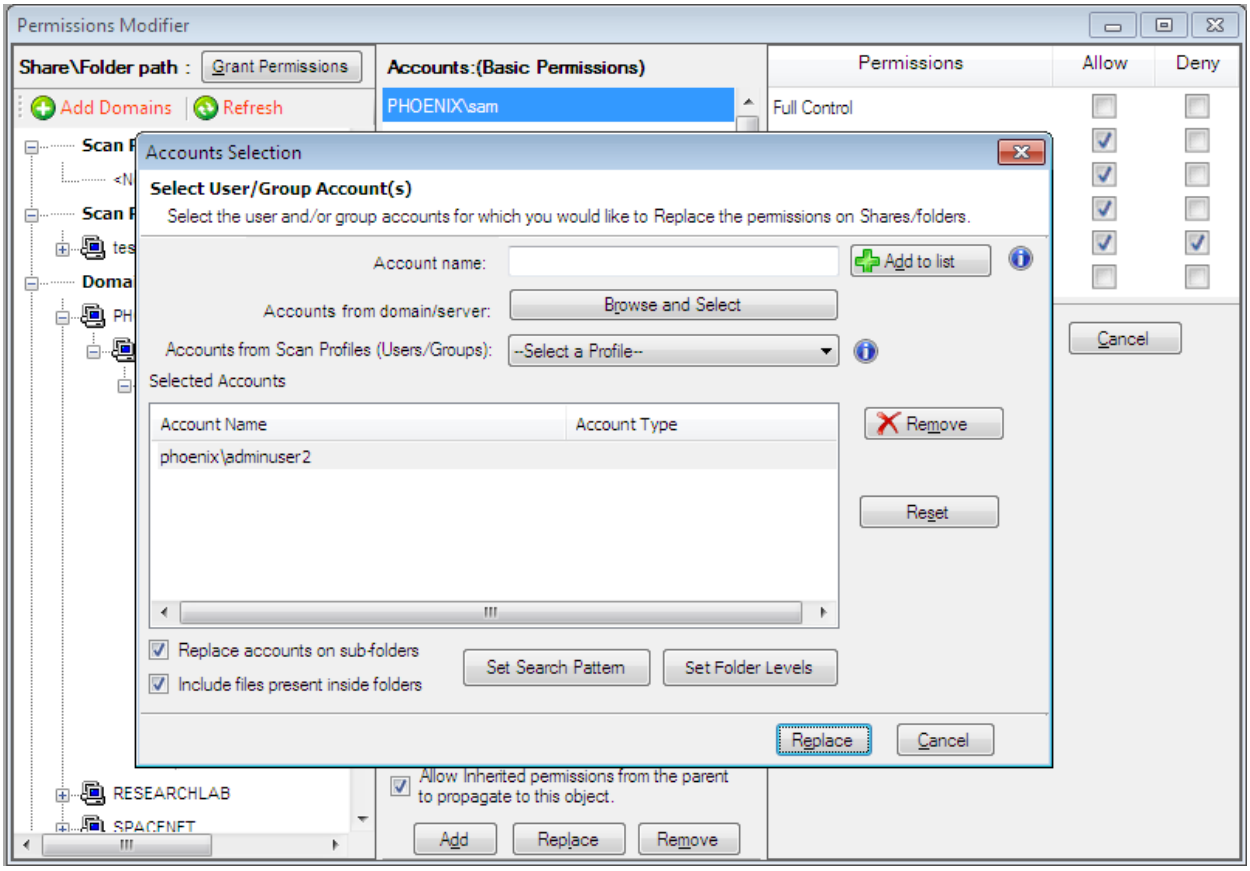
- Follow the list of options to enumerate the shared folder/file as outlined in How to enumerate shared folders/files?

Step 2: Select an account and click Replace

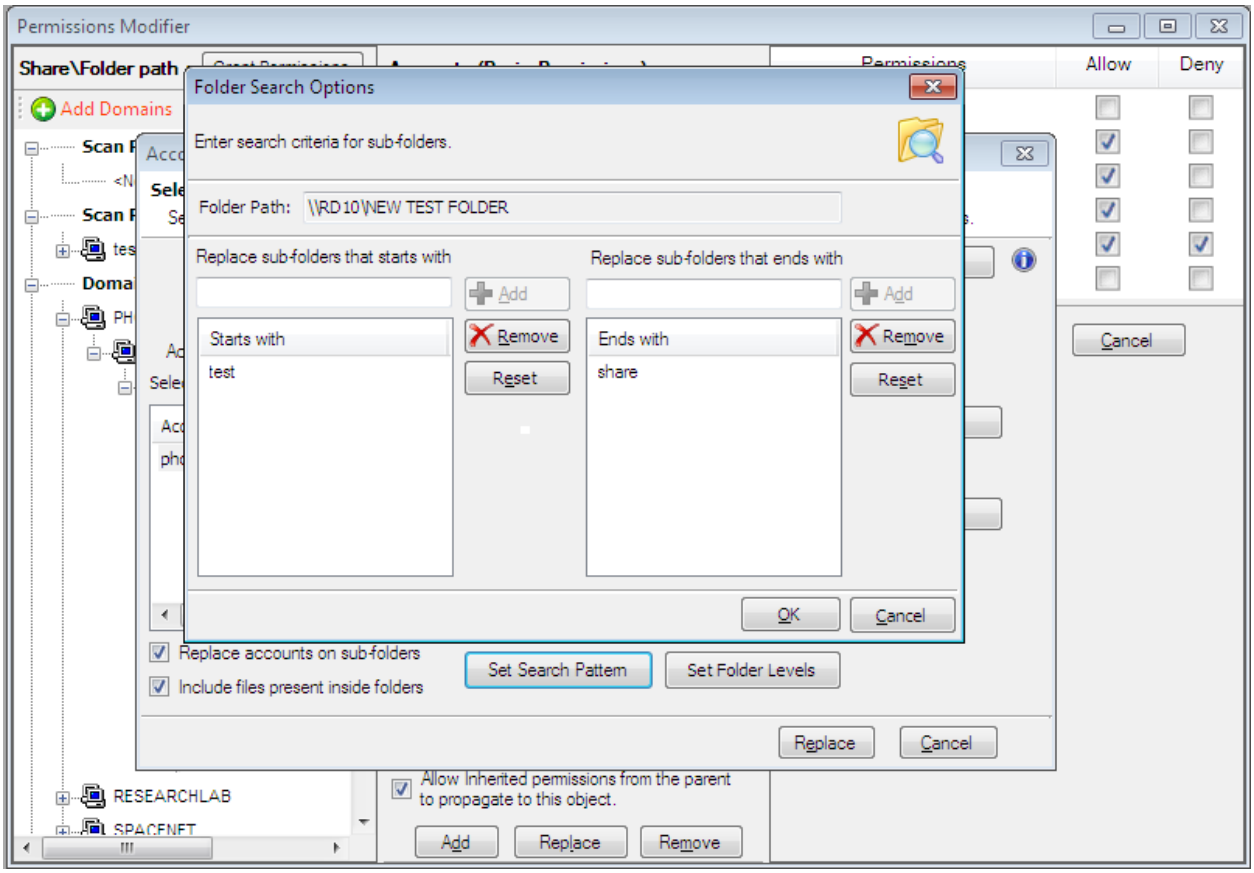
- Select an account from the Basic or Advanced permissions account list.
- Click **Replace** button. The Accounts Selection window will be displayed as shown below.



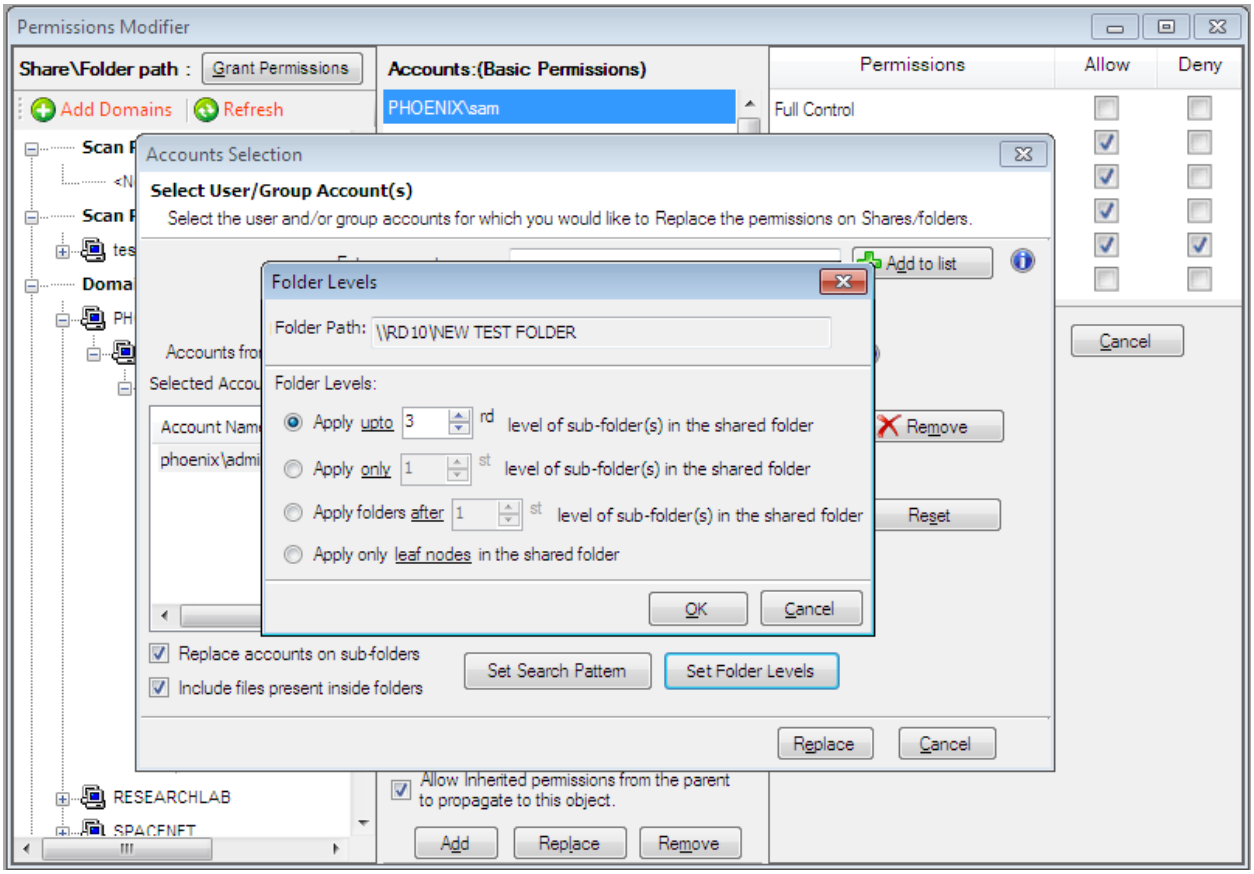
1. Select the user or group, for which you wish to replace the selected account in the folder/file permissions list.



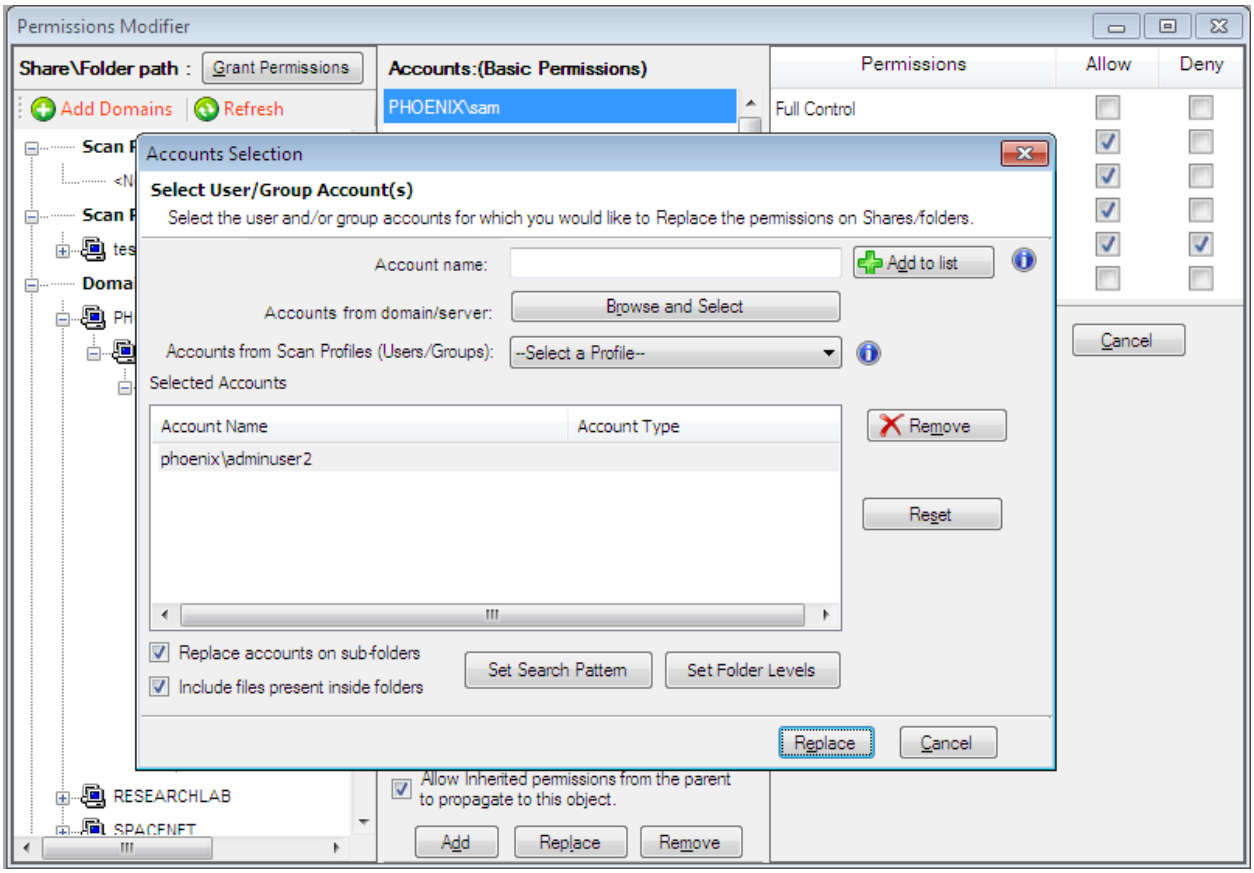
- **Replace accounts on sub-folders**: This option will replace accounts on sub-folders of the selected folder.
- **Include files present inside folders**: This option will replace accounts on files present inside the selected folder.
- Use **Set Search Pattern** option to perform replace permissions for sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example Folder name starts with test, Folder name ends with share.



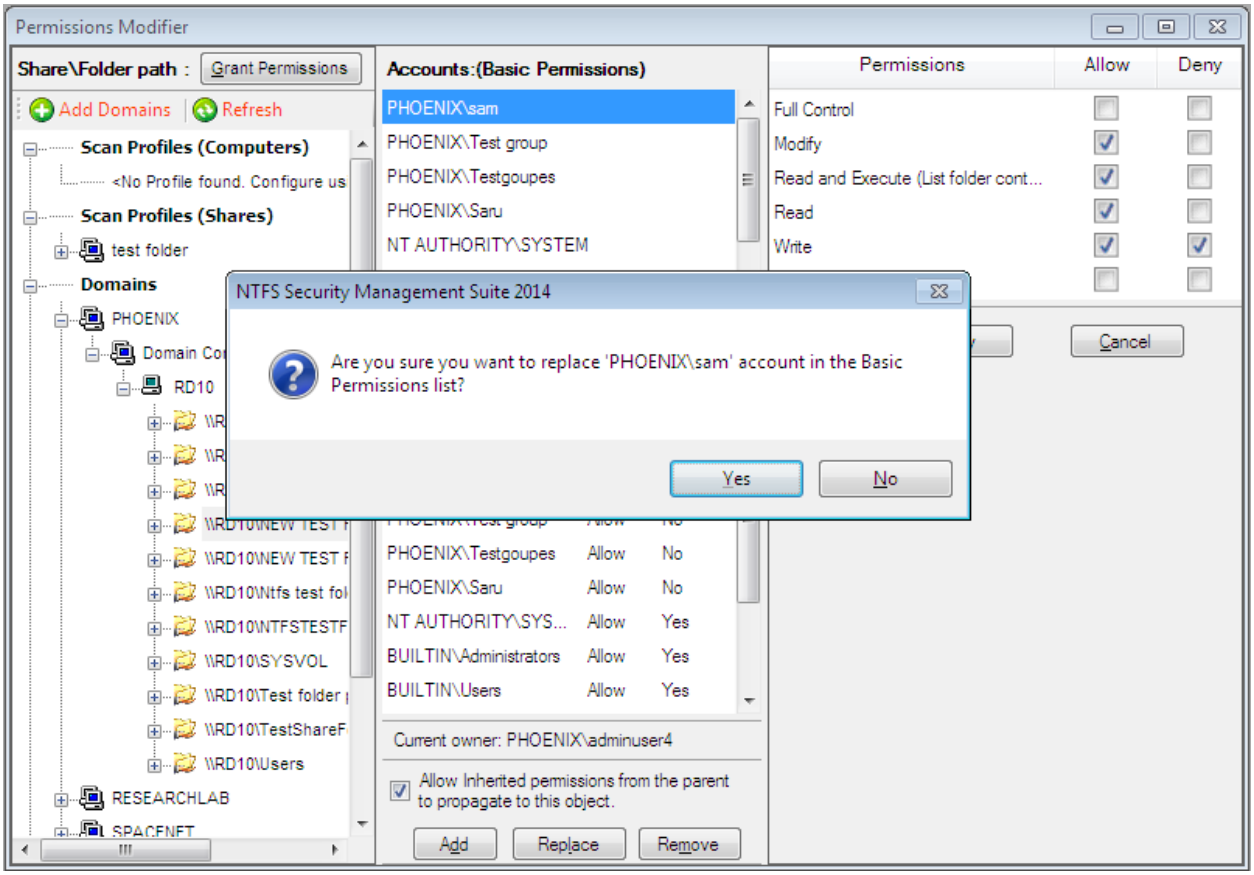
- Click **OK** button in the Folder Search Options window.
- Use **Set Folder Levels** option to replace the accounts in the selected levels of sub-folder(s) in the shared folder.



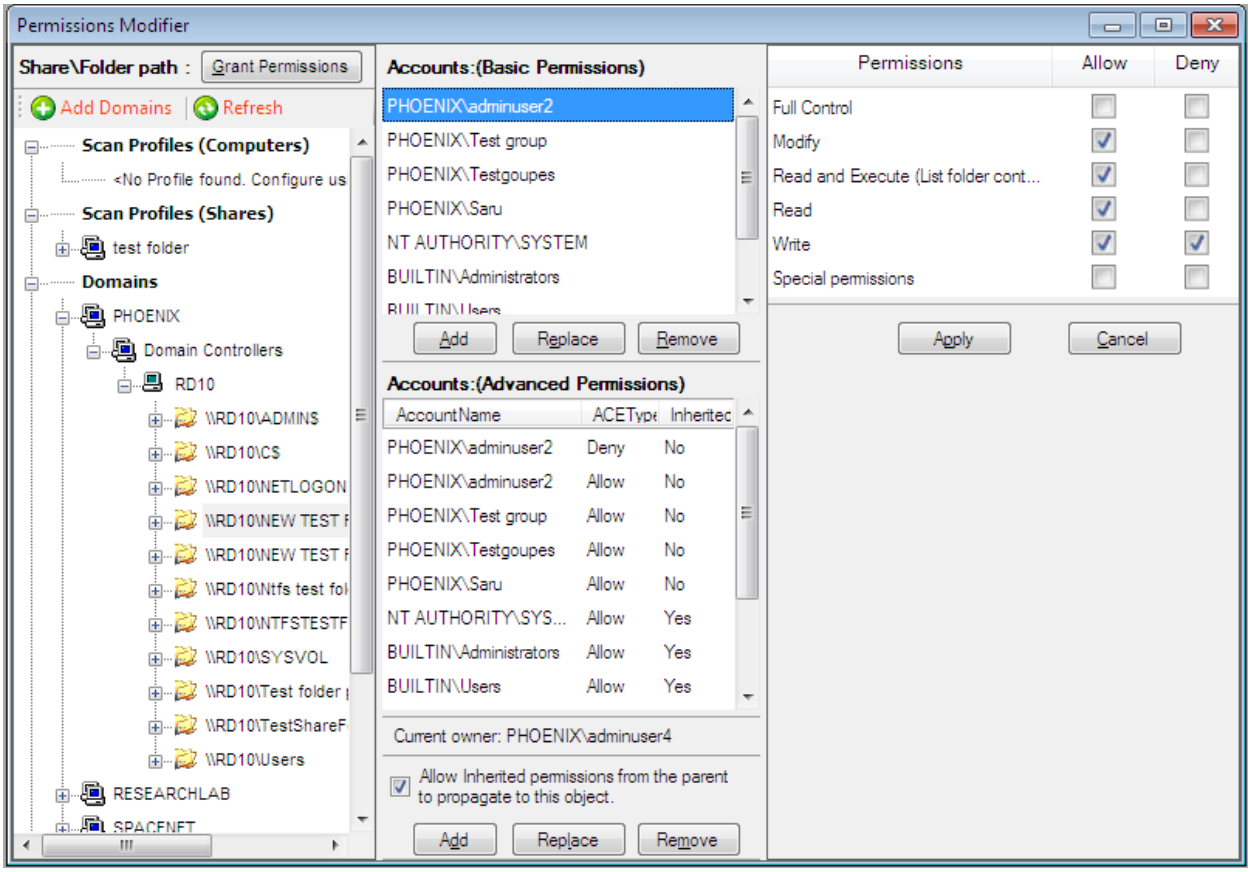
- **Apply upto N level(s) of sub-folder(s) in the shared folder:** This option will replace the account with the selected account on sub-folders which are upto specified folder traversal level.
- **Apply only Nth level of sub-folder(s) in the shared folder:** This option will replace the account in sub-folders which are in the specified traversal level only.
- **Apply folders after N level(s) of sub-folder(s) in the shared folder:** This option will replace the account in sub-folders which are after the nth traversal level of the selected folder.
- **Apply only leaf nodes in the shared folder:** This option will replace the account with the selected account in the last child leaf nodes without affecting the parent folder's permissions.
- Click **OK** button in the Folder Levels window. The Accounts Selection window will be displayed as shown below:



- Click **Replace** button in the Accounts Selection window.

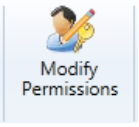


- Click **Yes** to replace the selected account.
- The updated permissions list will be displayed as shown below:


Permissions Modifier
Share\Folder path :
Grant Permissions
Add Domains
Refresh
Scan Profiles (Computers)
<No Profile found. Configure us
Scan Profiles (Shares)
test folder
Domains
PHOENIX
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST F
\\RD10\NEW TEST F
\\RD10\Ntfs test fol
\\RD10\NTFSTESTF
\\RD10\SYSVOL
\\RD10\Test folder
\\RD10\TestShareF
\\RD10\Users
RESEARCHLAB
SPACENET
Accounts:(Basic Permissions)
PHOENIX\adminuser2
PHOENIX\Test group
PHOENIX\Testgoupes
PHOENIX\Saru
NT AUTHORITY\SYSTEM
BUILTIN\Administrators
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
PHOENIX\adminuser2 Deny No
PHOENIX\adminuser2 Allow No
PHOENIX\Test group Allow No
PHOENIX\Testgoupes Allow No
PHOENIX\Saru Allow No
NT AUTHORITY\SYS... Allow Yes
BUILTIN\Administrators Allow Yes
BUILTIN\Users Allow Yes
Current owner: PHOENIX\adminuser4
Allow Inherited permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Full Control
Modify
Read and Execute (List folder cont...
Read
Write
Special permissions
Apply
Cancel

How to remove the selected account from the shared folder/file permissions list?

The **Modify Permissions** feature allows you to remove the selected account and its permissions from folder/file permissions list.

Click on 

button.

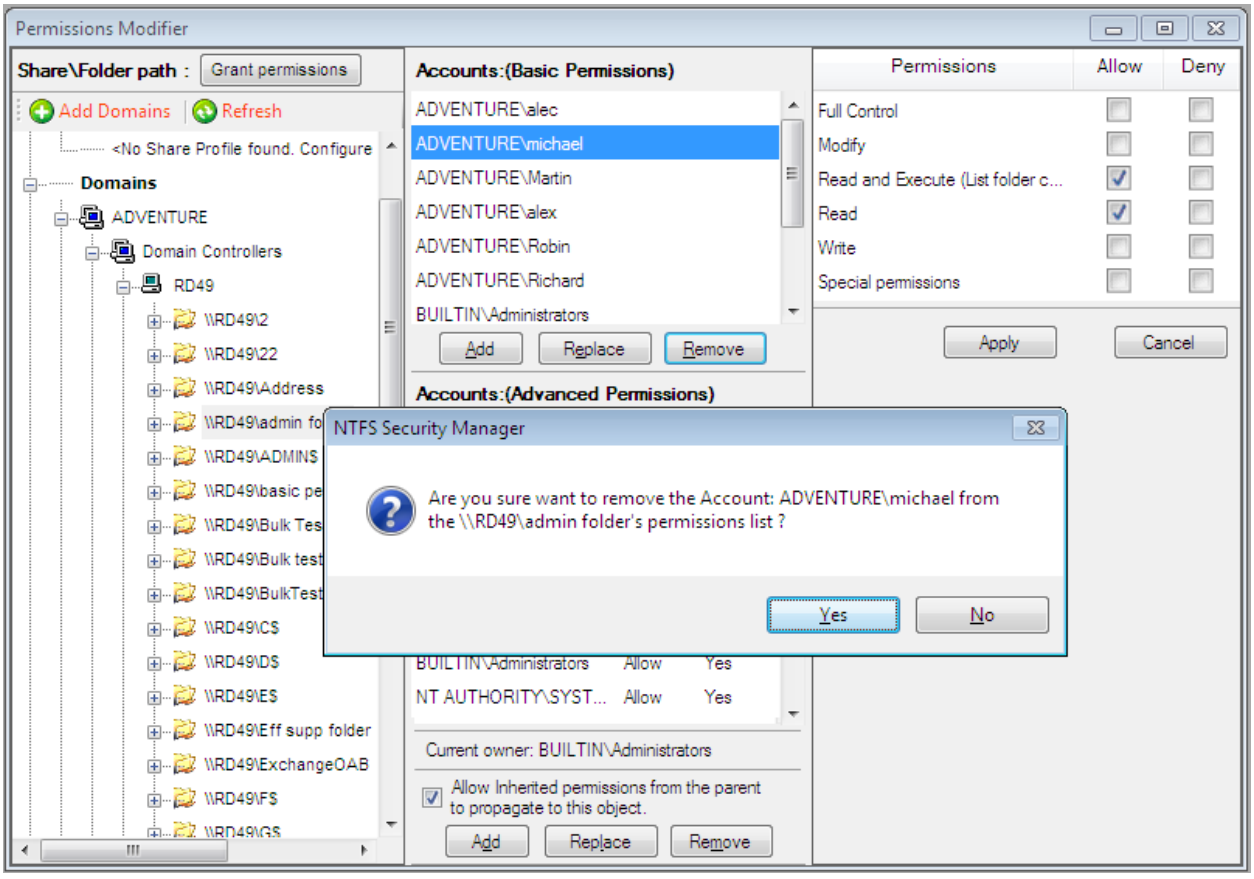
The Modify Permissions window will be displayed.

Step 1: Select folder/file path

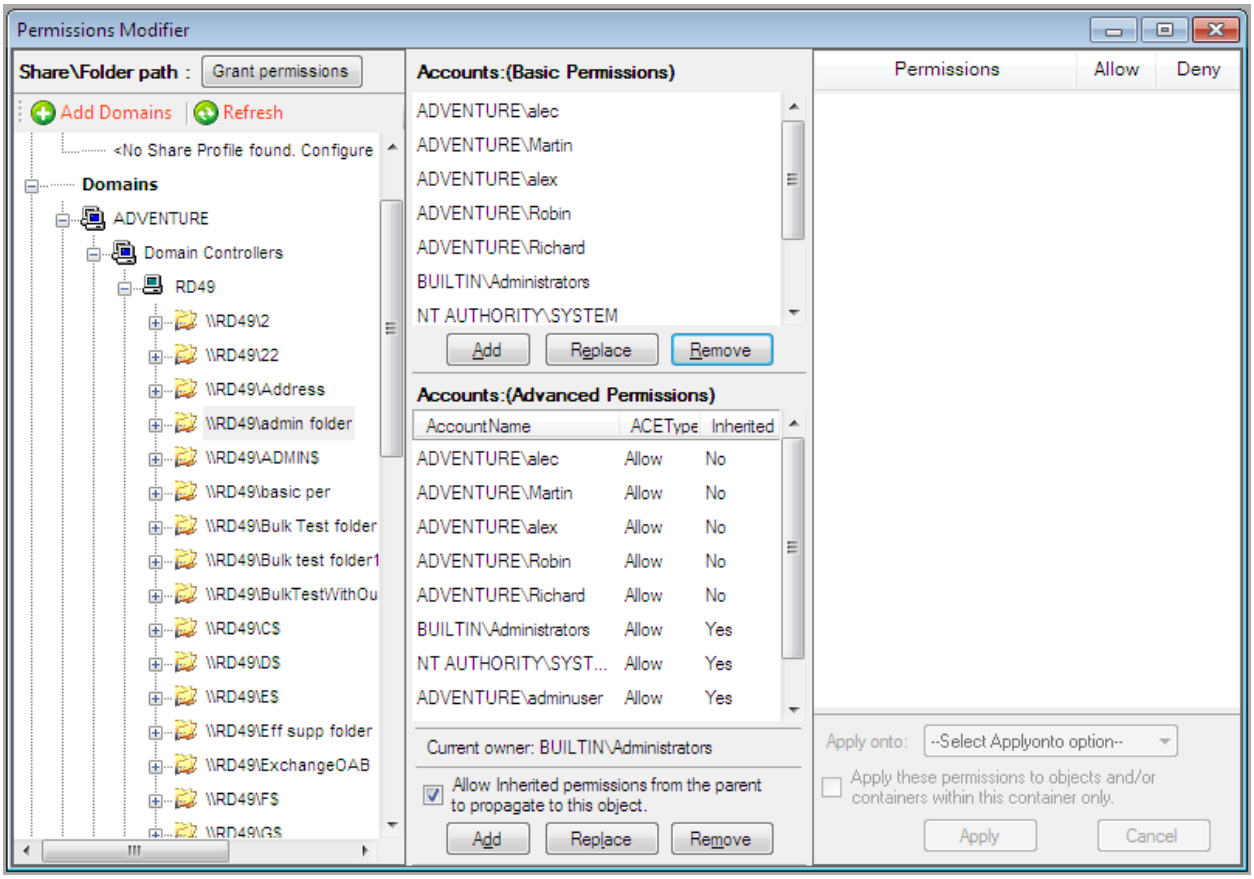
- Follow the list of options to enumerate the shared folders/files as outlined in -share.htm"How to enumerate shared folders/files?

Step 2: Select an account and Click Remove

- Select an account from the Basic or Advanced permissions Account list.
- Click **Remove**.

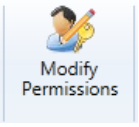


- Click **Yes** to remove the selected Account.
- The updated permissions list will be displayed as shown below:



How to allow inheritance from the parent to current folder/file permissions?

You may use the **Permissions Modifier** to allow inherited permissions from the parent to the current folder/file permissions.

Click on 

button.

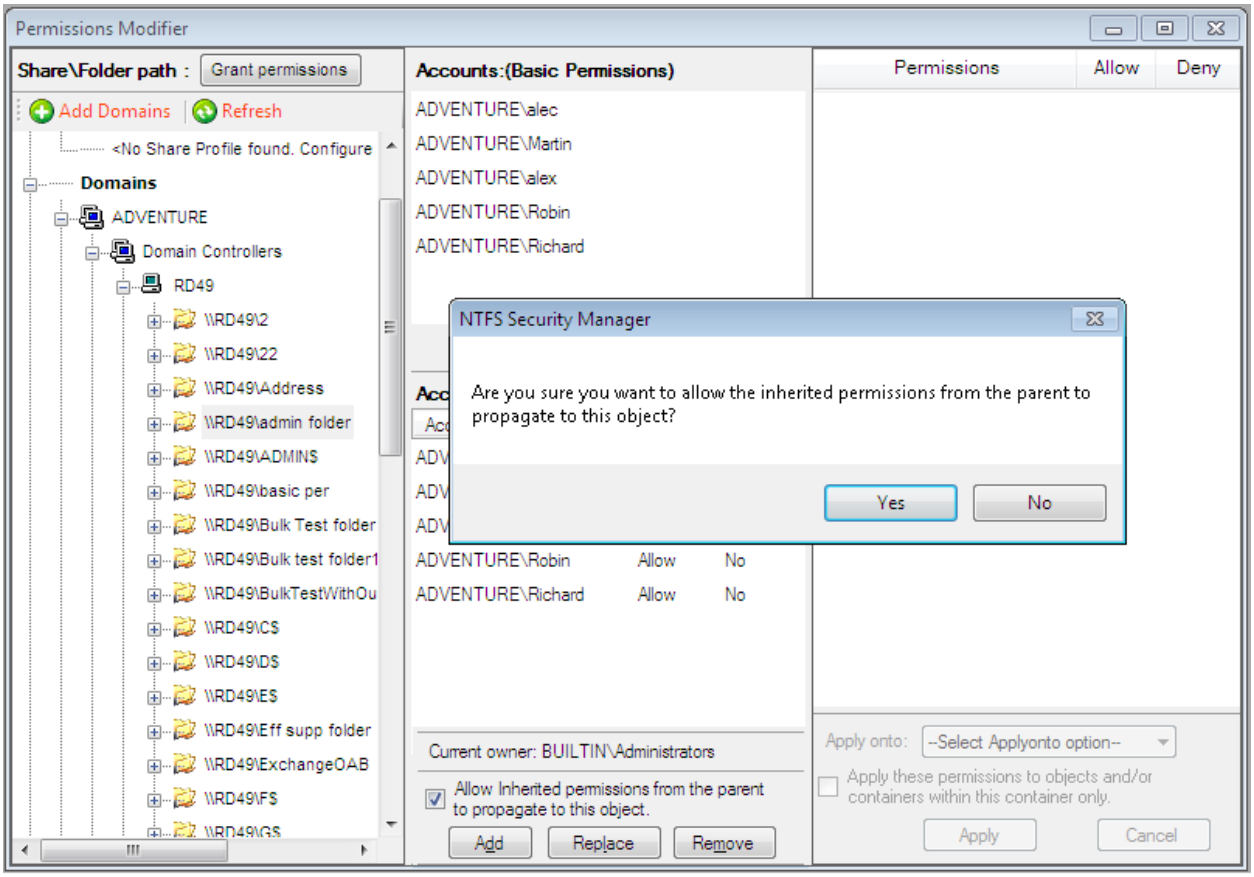
The Modify Permissions window will be displayed as shown below:

Step 1: Select folder/file path

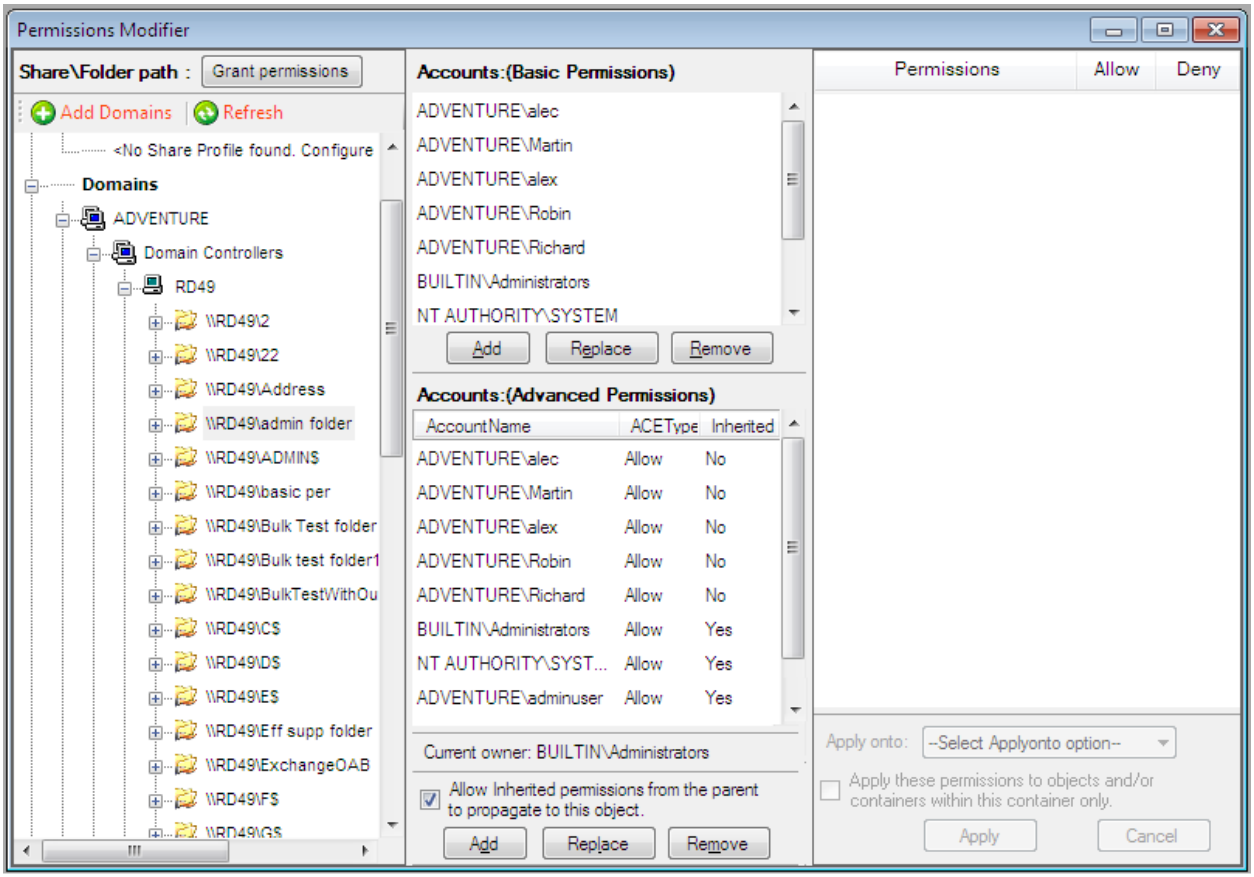
- Follow the list of options to enumerate the shared folders/files as outlined in How to enumerate shared folders/files?

Step 2: Check Allow inheritance

- Check the option **Allow inherited permissions from the parent to propagate to this object**.

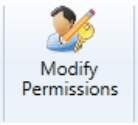


- Click **Yes** to allow inheritance.
- The updated permissions list with inherited permissions from the parent object as shown below:


Permissions Modifier
Share\Folder path :
Grant permissions
Add Domains
Refresh
<No Share Profile found. Configure
Domains
ADVENTURE
Domain Controllers
RD49
\\RD49\2
\\RD49\22
\\RD49\Address
\\RD49\admin folder
\\RD49\ADMIN$
\\RD49\basic per
\\RD49\Bulk Test folder
\\RD49\Bulk test folder1
\\RD49\BulkTestWithOu
\\RD49\C$
\\RD49\D$
\\RD49\E$
\\RD49\Eff supp folder
\\RD49\ExchangeOAB
\\RD49\F$
Accounts:(Basic Permissions)
ADVENTURE\alec
ADVENTURE\Martin
ADVENTURE\alex
ADVENTURE\Robin
ADVENTURE\Richard
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
ADVENTURE\alec Allow No
ADVENTURE\Martin Allow No
ADVENTURE\alex Allow No
ADVENTURE\Robin Allow No
ADVENTURE\Richard Allow No
BUILTIN\Administrators Allow Yes
NT AUTHORITY\SYST... Allow Yes
ADVENTURE\adminuser Allow Yes
Current owner: BUILTIN\Administrators
Allow Inherited permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Apply onto:
--Select Applyonto option--
Apply these permissions to objects and/or containers within this container only.
Apply
Cancel

How to block inheritance from the parent to the current folder/file permissions?

The **Permissions Modifier** allows you to block inherited permissions from the parent to the current folder/file permissions.

Click on 

button.

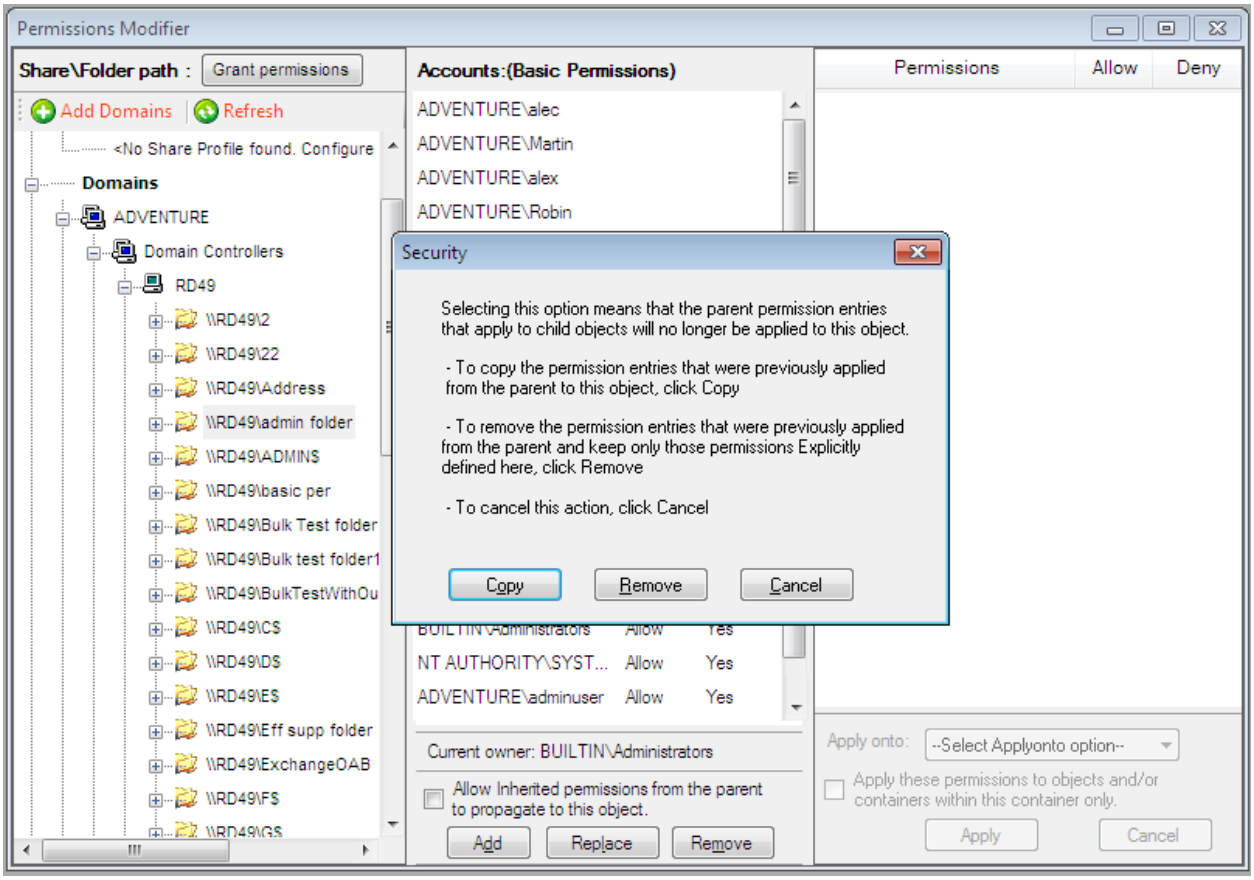
The Modify Permissions window will be displayed.

Step 1: Select folder/file path

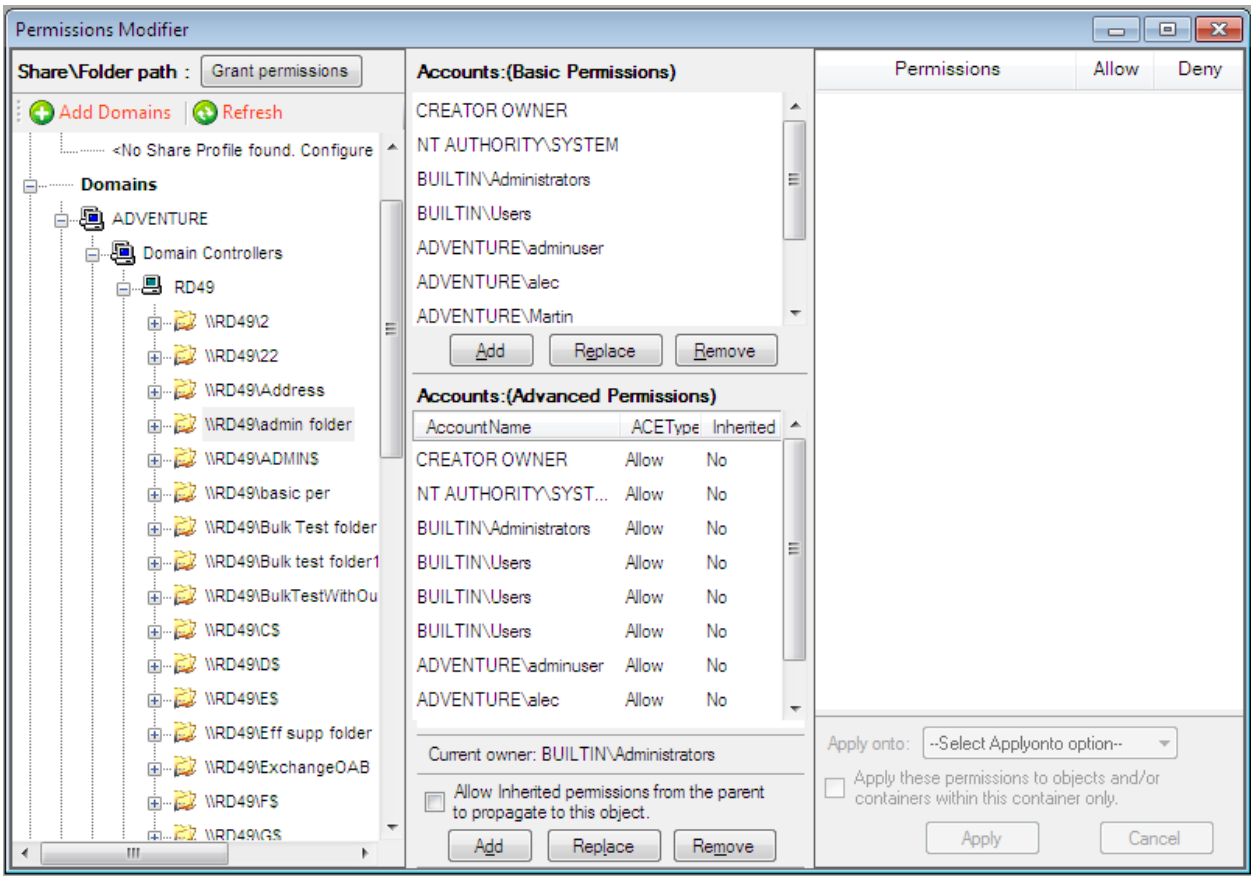
- Follow the list of options to enumerate the shared folders/files as outlined in -share.htm">How to enumerate shared folders/files?

Step 2: Uncheck Allow inheritance

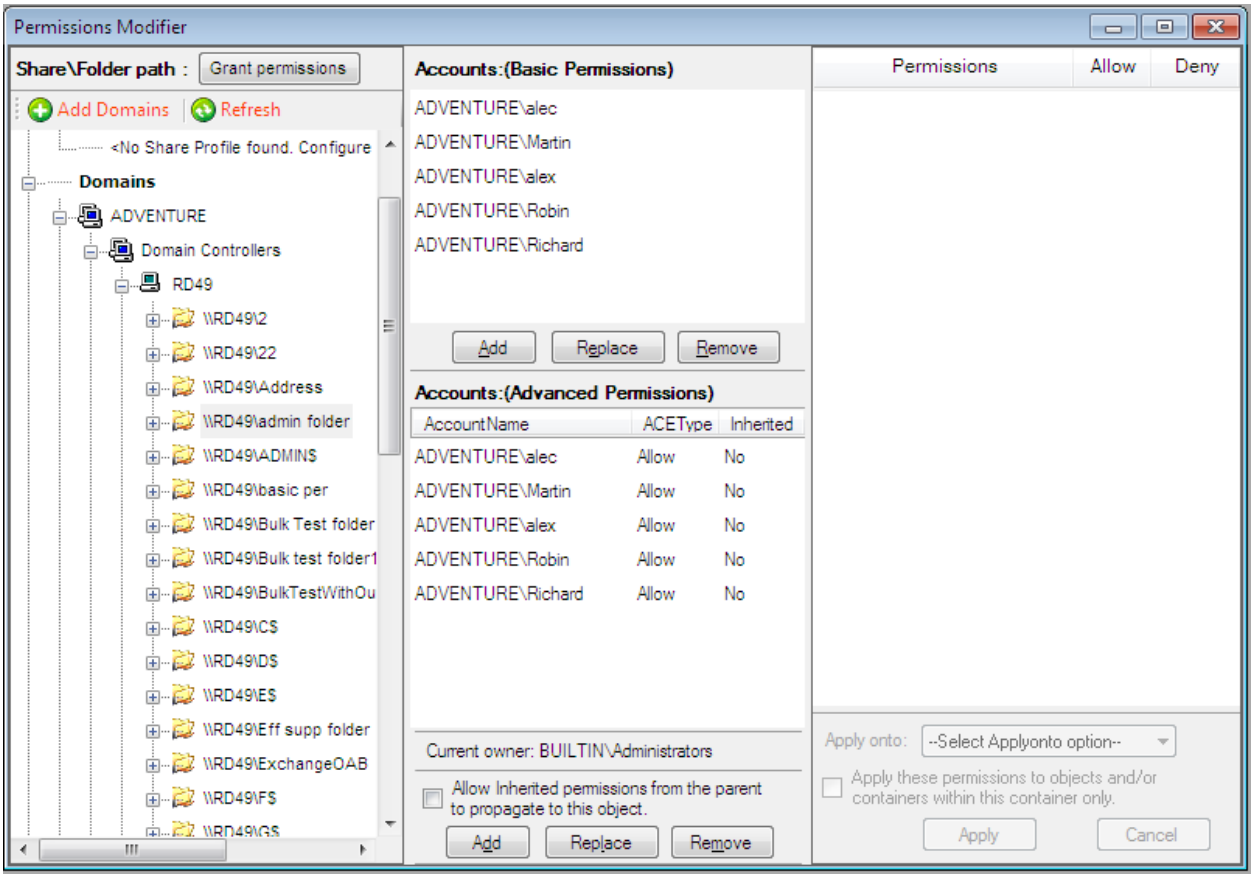
- Uncheck the option **Allow inherited permissions from the parent to propagate to this object**.



- Click the option **Copy** to copy all the permissions entries that were previously inherited from the parent to this current shared folder(s)/files permissions list.
- The updated permissions list with copied permissions from the parent object as shown below:

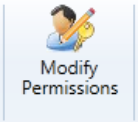


- Click the option **Remove** to Remove the permission entries that were previously inherited from the parent and keep only those permissions explicitly defined/granted this current shared folder(s)/file(s).
- The updated permissions list after removing the inherited permissions from the parent object as shown below:


Permissions Modifier
Share\Folder path :
Grant permissions
Add Domains
Refresh
<No Share Profile found. Configure
Domains
ADVENTURE
Domain Controllers
RD49
\\RD49\2
\\RD49\22
\\RD49\Address
\\RD49\admin folder
\\RD49\ADMIN$
\\RD49\basic per
\\RD49\Bulk Test folder
\\RD49\Bulk test folder1
\\RD49\BulkTestWithOu
\\RD49\C$
\\RD49\D$
\\RD49\E$
\\RD49\Eff supp folder
\\RD49\ExchangeOAB
\\RD49\F$
Accounts:(Basic Permissions)
ADVENTURE\alec
ADVENTURE\Martin
ADVENTURE\alex
ADVENTURE\Robin
ADVENTURE\Richard
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
ADVENTURE\alec Allow No
ADVENTURE\Martin Allow No
ADVENTURE\alex Allow No
ADVENTURE\Robin Allow No
ADVENTURE\Richard Allow No
Current owner: BUILTIN\Administrators
Allow Inheritied permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Apply onto:
--Select Applyonto option--
Apply these permissions to objects and/or containers within this container only.
Apply
Cancel

How to modify an account Basic permissions?

The **Modify Permissions** allows you to modify an account's Basic permissions.

Click on 

button.

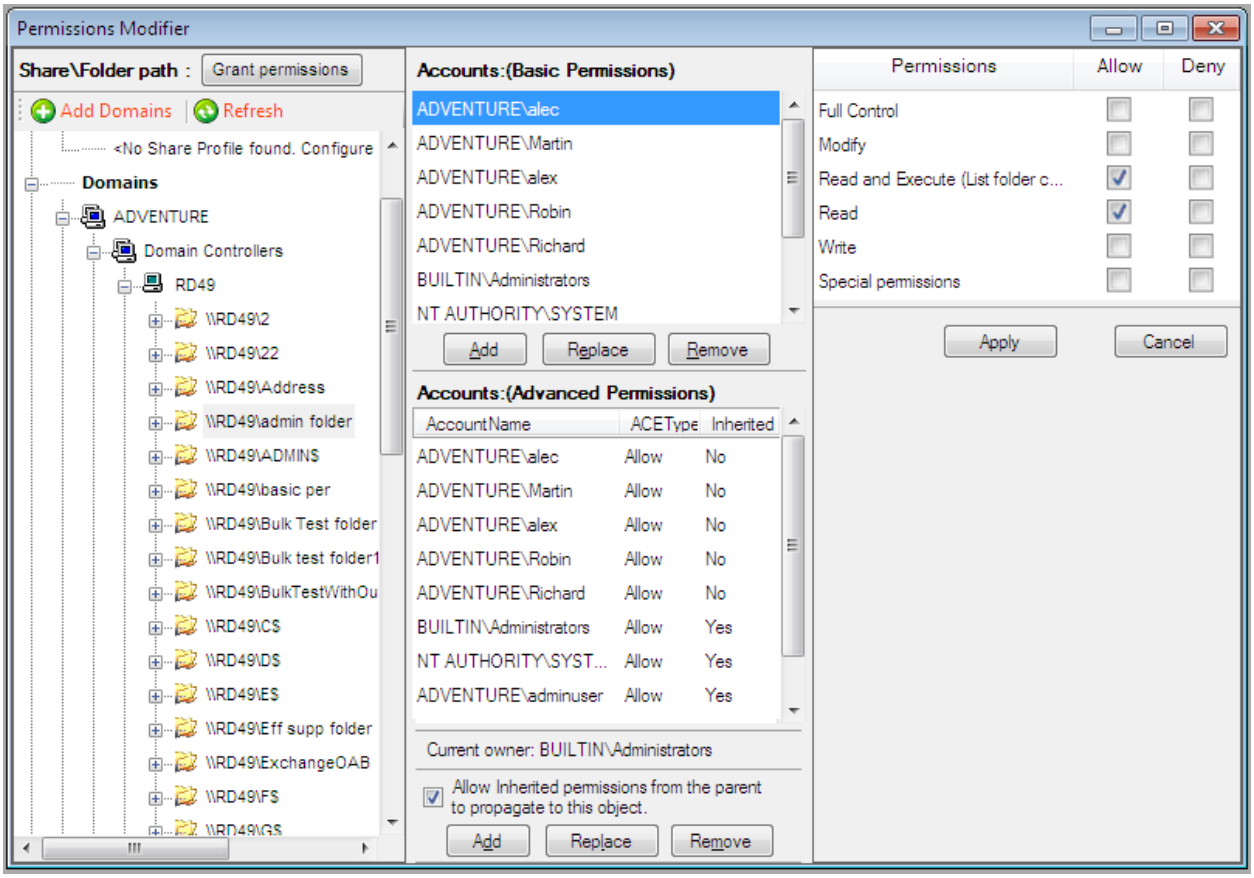
The Modify Permissions window will be displayed.

Step 1: Select folder/file path

- Follow the list of options to enumerate the shared folders/files as outlined in How to enumerate shared folders/files?

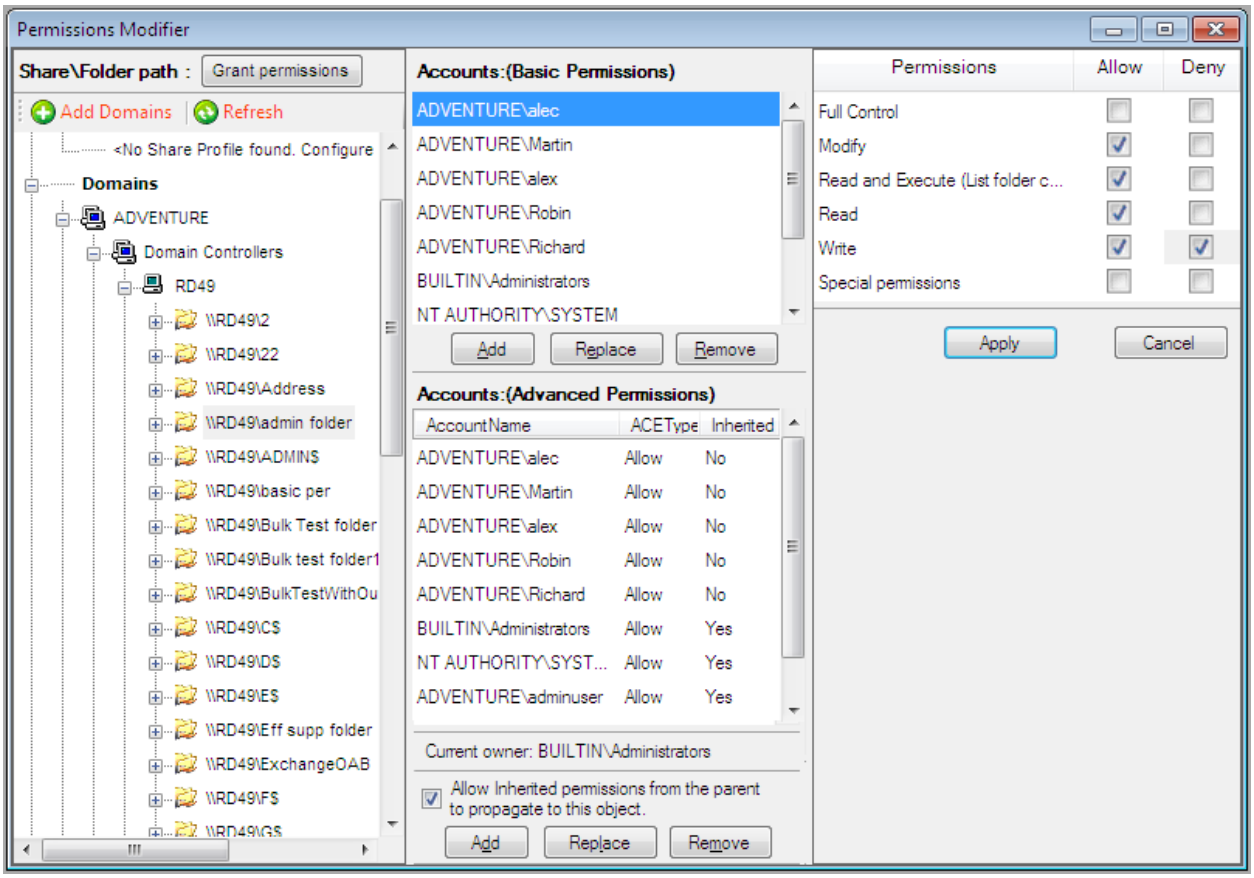
Step 2: Select an Account

Select an account in the Basic permissions to modify its permissions.

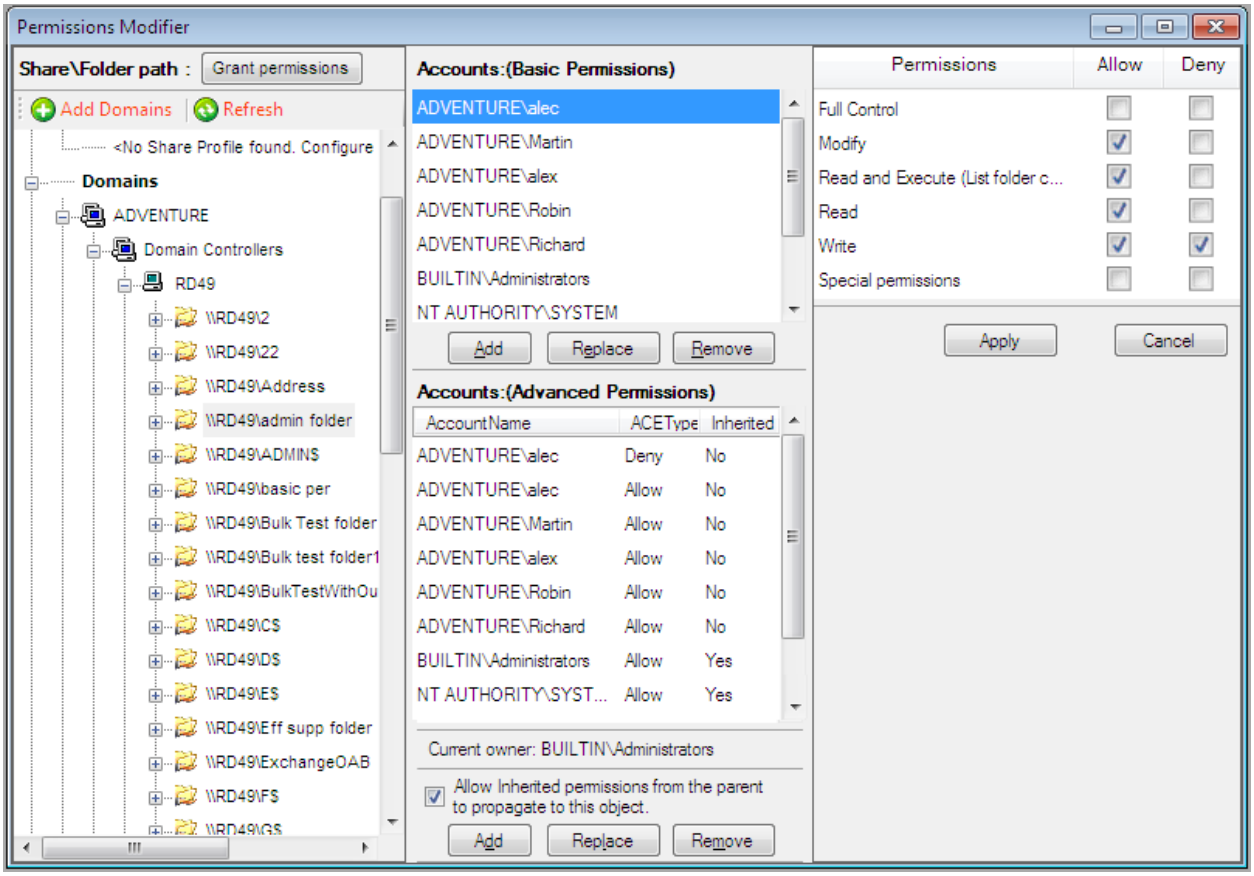


- Check the permissions you want to add and uncheck the permissions you want to remove, in the permissions column.
- Click the button **Apply** to update the basic permissions for the selected account

Caution: If all the permissions are unchecked, the account will be completely removed from the ACE list.

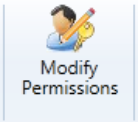


- The updated basic permissions for the selected account as shown below.


Permissions Modifier
Share\Folder path :
Grant permissions
Add Domains
Refresh
<No Share Profile found. Configure
Domains
ADVENTURE
Domain Controllers
RD49
\\RD49\2
\\RD49\22
\\RD49\Address
\\RD49\admin folder
\\RD49\ADMIN$
\\RD49\basic per
\\RD49\Bulk Test folder
\\RD49\Bulk test folder1
\\RD49\BulkTestWithOu
\\RD49\C$
\\RD49\D$
\\RD49\E$
\\RD49\Eff supp folder
\\RD49\ExchangeOAB
\\RD49\F$
Accounts:(Basic Permissions)
ADVENTURE\alec
ADVENTURE\Martin
ADVENTURE\alex
ADVENTURE\Robin
ADVENTURE\Richard
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
ADVENTURE\alec Deny No
ADVENTURE\alec Allow No
ADVENTURE\Martin Allow No
ADVENTURE\alex Allow No
ADVENTURE\Robin Allow No
ADVENTURE\Richard Allow No
BUILTIN\Administrators Allow Yes
NT AUTHORITY\SYST... Allow Yes
Current owner: BUILTIN\Administrators
Allow Inherited permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Full Control
Modify
Read and Execute (List folder c...
Read
Write
Special permissions
Apply
Cancel

How to modify an account Advanced permissions?

The **Modify Permissions** allows you to modify an account advanced permissions.

Click on 

button.

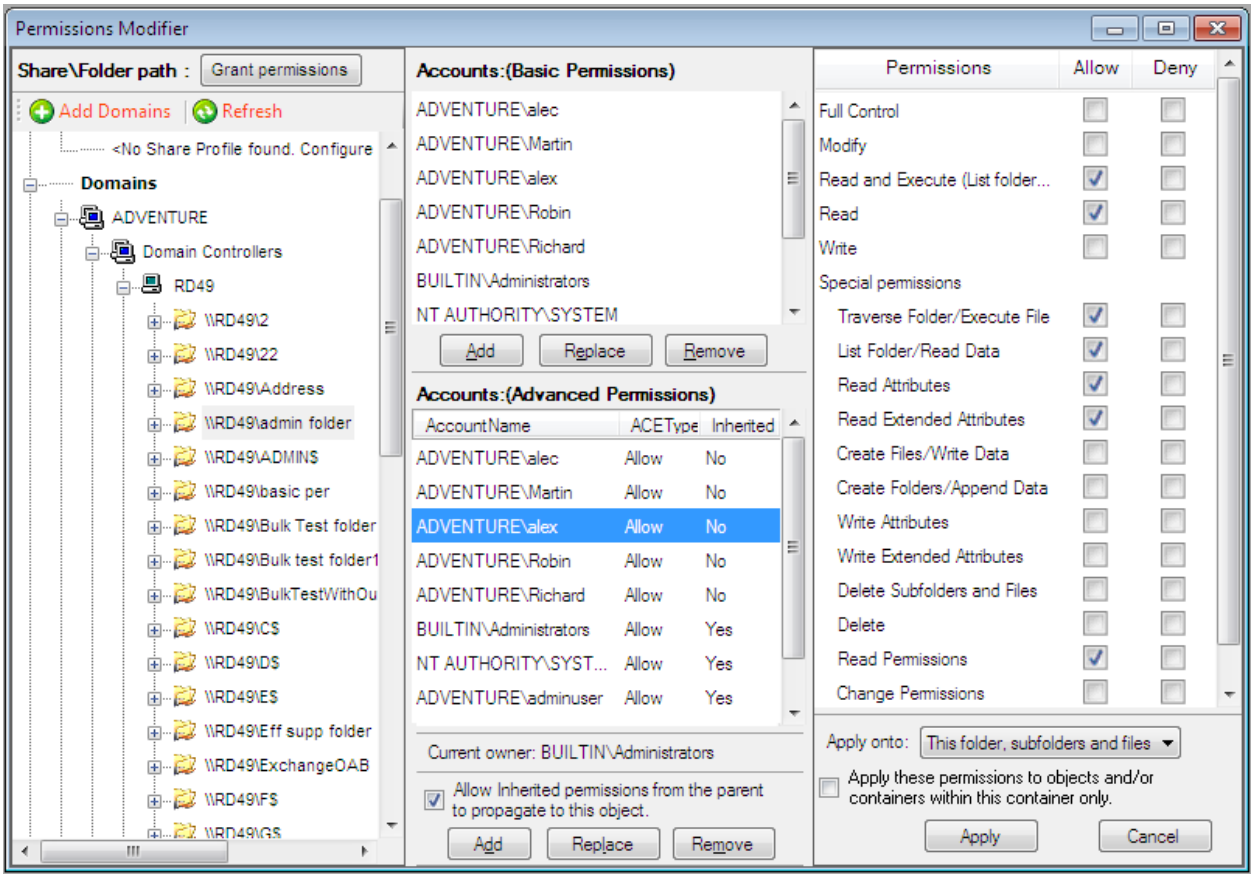
The Modify Permissions window will be displayed as shown below:

Step 1: Select folder/file path

- Follow the list of options to enumerate the shared folders/files as outlined in How to enumerate shared folders/files?

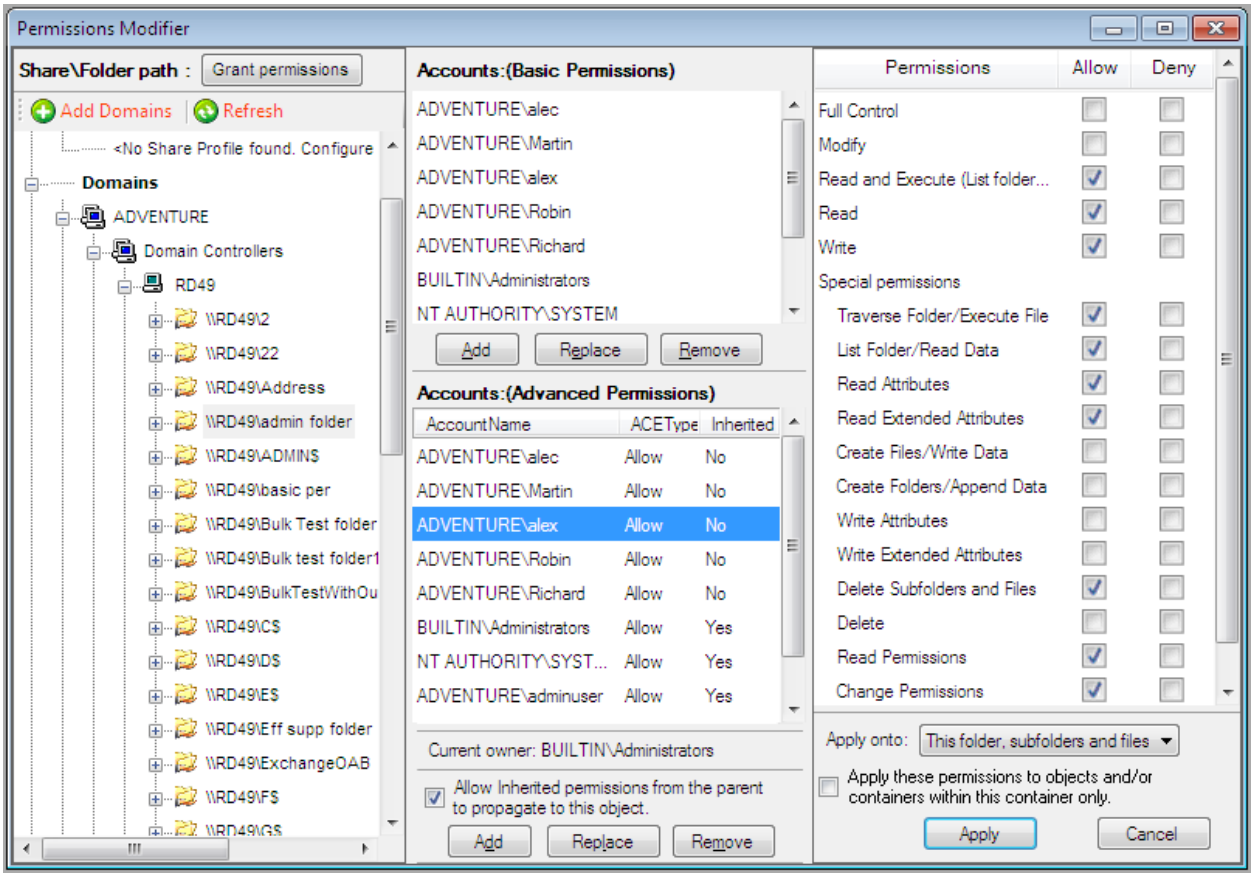
Step 2: Select an Account

Select the Advanced permissions account for which you want to modify the permissions.

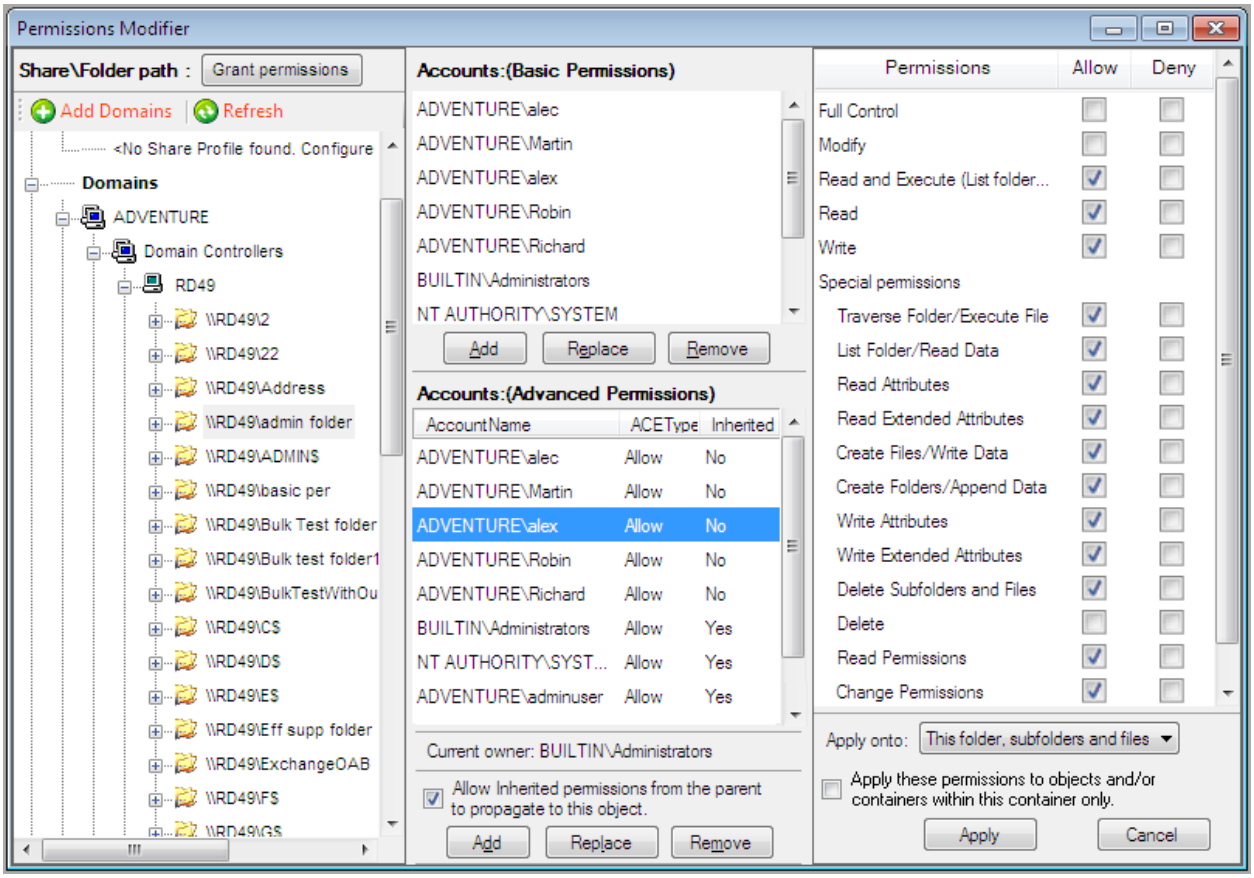


- Check the permissions you want to add and uncheck the permissions you want to remove from the account's advanced permissions.
- Click the button **Apply** to update the advanced permissions for the selected account.
- You can also modify the propagation level to all it's subfolders and files by using the option **Apply onto**.

Caution: If all the permissions are unchecked, the account will be completely removed from the ACE list.



- The updated advanced permissions for the selected account as shown below.


Permissions Modifier
Share\Folder path :
Grant permissions
Add Domains
Refresh
<No Share Profile found. Configure
Domains
ADVENTURE
Domain Controllers
RD49
\\RD49\2
\\RD49\22
\\RD49\Address
\\RD49\admin folder
\\RD49\ADMIN$
\\RD49\basic per
\\RD49\Bulk Test folder
\\RD49\Bulk test folder1
\\RD49\BulkTestWithOu
\\RD49\C$
\\RD49\D$
\\RD49\E$
\\RD49\Eff supp folder
\\RD49\ExchangeOAB
\\RD49\F$
Accounts:(Basic Permissions)
ADVENTURE\alec
ADVENTURE\Martin
ADVENTURE\alex
ADVENTURE\Robin
ADVENTURE\Richard
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
Add
Replace
Remove
Accounts:(Advanced Permissions)
AccountName
ACEType
Inherited
ADVENTURE\alec Allow No
ADVENTURE\Martin Allow No
ADVENTURE\alex Allow No
ADVENTURE\Robin Allow No
ADVENTURE\Richard Allow No
BUILTIN\Administrators Allow Yes
NT AUTHORITY\SYST... Allow Yes
ADVENTURE\adminuser Allow Yes
Current owner: BUILTIN\Administrators
Allow Inherited permissions from the parent to propagate to this object.
Add
Replace
Remove
Permissions
Allow
Deny
Full Control
Modify
Read and Execute (List folder...
Read
Write
Special permissions
Traverse Folder/Execute File
List Folder/Read Data
Read Attributes
Read Extended Attributes
Create Files/Write Data
Create Folders/Append Data
Write Attributes
Write Extended Attributes
Delete Subfolders and Files
Delete
Read Permissions
Change Permissions
Apply onto:
This folder, subfolders and files
Apply these permissions to objects and/or containers within this container only.
Apply
Cancel

Copy Permissions

About Copy Permissions

How to Copy Permissions from one share to another share(s)?

How to reuse the Copy Permission s template?

About Copy Permissions

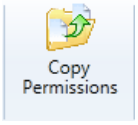
The **Copy Permissions** feature allows you to copy permissions from one share to another share(s). You can use many options like Add the new permissions to the account's existing permissions, Replace the account's existing permissions with the new permissions, etc. You may select options to Allow, Block inheritance from the parent object and also Replace all child objects existing permissions with the inheritable permissions from this object while copying permissions to share. Here is the list of actions you can perform using the Copy Permissions feature.

Note: This feature will not break the inheritance from the parent of target object. If you still wish to break the inheritance from the parent object, you may use the option "Block Inherited permissions from this object's parent" to block inheritance.

Actions
Copy permissions from one share to another share(s): (How to?)
Copy source shared folder/file permissions to the selected target shared folder(s)/file(s) permissions list.
Replace existing accounts permissions with the new permissions: (How to?)
Replace the existing accounts permissions, If an existing account is selected to copy permissions to a target shared folder/file.
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files): (How to?)
Copy permissions to the target object's subfolders and files that do not have inherited permissions from its parent object with respect to the above options.
Remove all the existing explicit accounts and replace with the new accounts: (How to?)
Remove all existing accounts that have explicitly assigned permissions for target shares and replace them with the selected accounts and permissions.
Replace all explicit permissions existing in descendant with the inherited permissions from the current object: (How to?)
Remove explicitly defined permissions on all descendant objects and replace them with the inheritable permissions from the target shared folder(s)/file(s) permissions list.
Allow inherited permissions from the parent object to the current shares: (How to?)
Allow inheritable permissions from the parent object to the target shares. It will not affect the already existing explicit permissions.
Copy and Remove inherited permissions from the parent object to the current shares: (How to?)
Copy and Remove the inheritable permissions from the parent object to the target shares. Copying the inheritable permissions will add the inherited permissions as explicit permissions in the target shares permissions list. Removing the inherited permissions will remove all the inherited permissions from the parent to the target object.

How to replace existing accounts permissions with the new permissions?

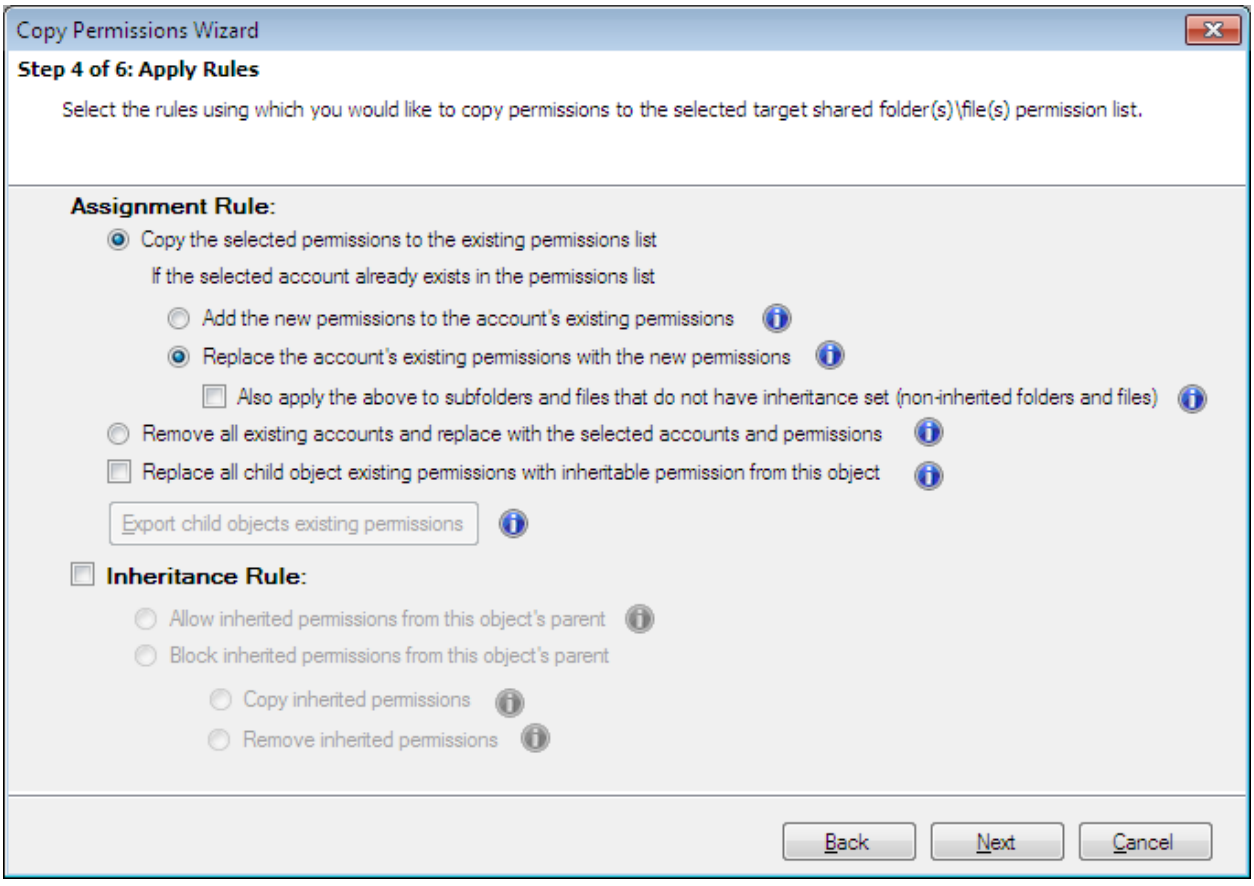
The **Copy Permissions** feature allows you to replace the existing accounts permissions, If the existing account selected for copy permissions.

Click on 

button.

The Copy Permissions window will be displayed.

- Follow the steps 1 through 3 as outlined in How to Copy permissions from one share to another share(s)?
- In step 4 select the option Replace the account's existing permissions with the new permissions.

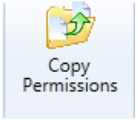

Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

Click **Next** to proceed to the next step.

Follow the steps 5 through 6 as outlined in How to Copy permissions from one share to another share(s)?

How to copy permissions to the target object's subfolders and files that do not have inherited permissions from its parent object?

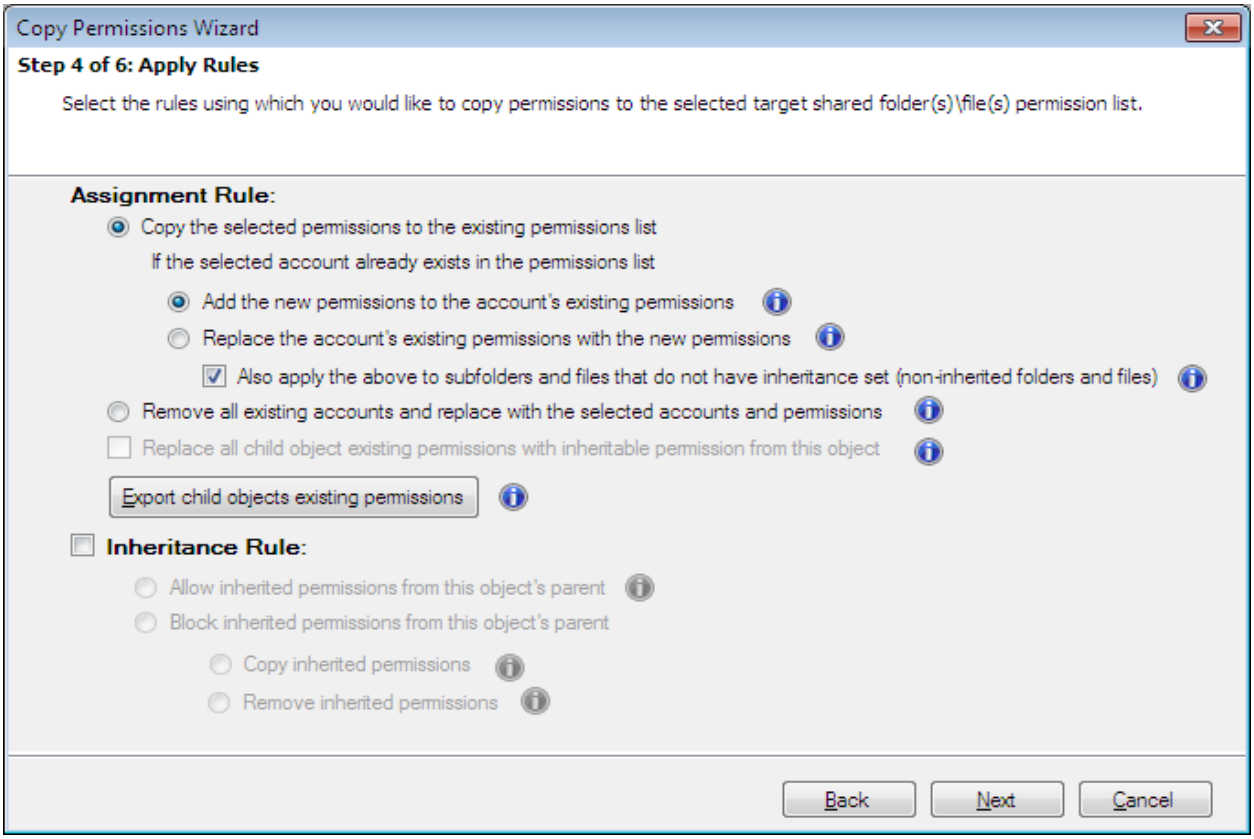
The **Copy Permissions** feature allows to copy permissions to the target object's subfolders and files that do not have inherited permissions from its parent object.

Click on 

button.

The Copy Permissions window will be displayed.

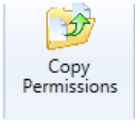
- Follow the steps 1 through 3 as outlined in How to Copy Permissions from one share to another share(s)?
- In step 4 select the option "Add the new permissions to the account's existing permissions" or "Replace the account's existing permissions with the new permissions"
- Then select the option **Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)**.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Copy Permissions from one share to another share(s)?

How to remove all the existing explicit accounts and replace with the new accounts?

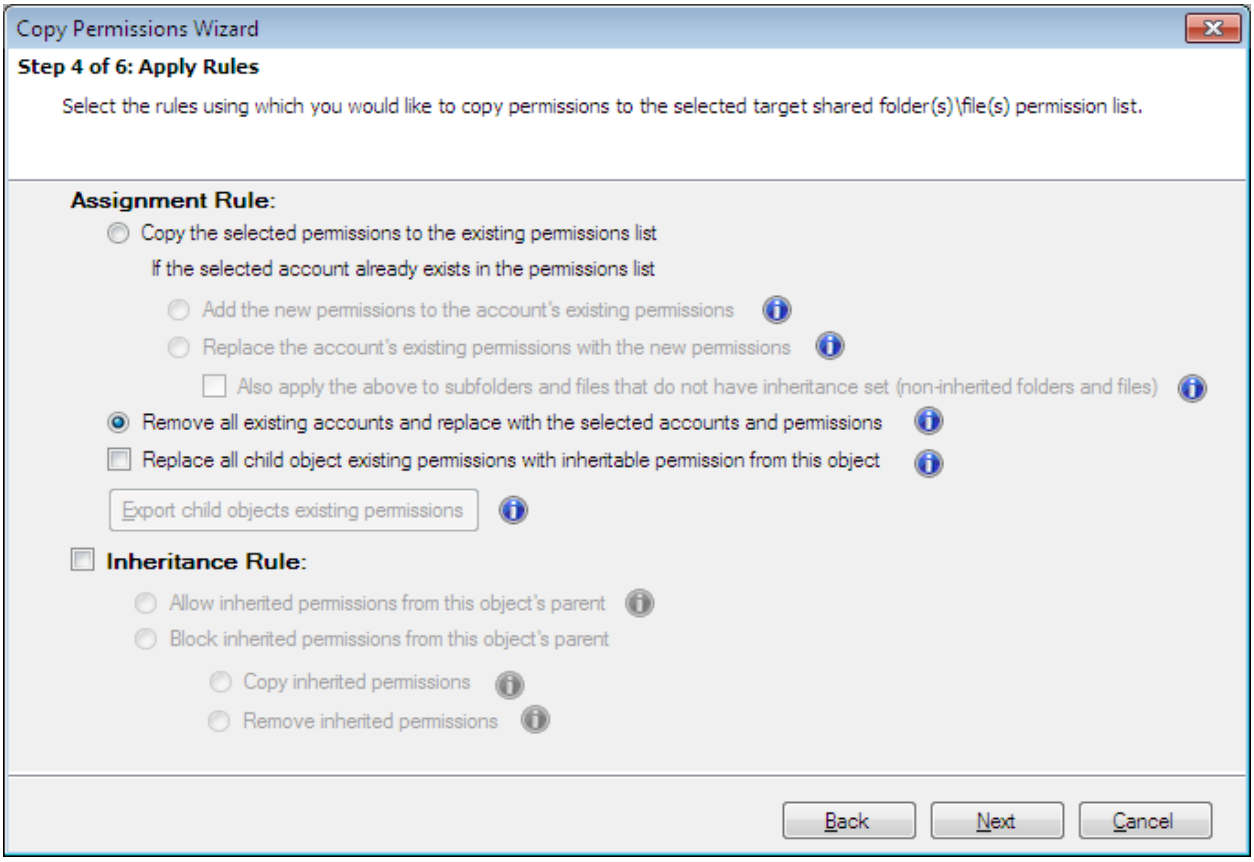
The **Copy Permissions** feature allows you to remove all existing accounts that have explicitly assigned permissions for shares and replace them with the selected accounts and permissions. Note that this will not remove inherited permissions from parent folder.

Click on 

button.

The Copy Permissions window will be displayed.

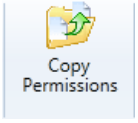
- Follow the steps 1 through 3 as outlined in How to Copy Permissions from one share to another share(s)?
- In step 4 select the option **Remove all existing accounts and replace with the selected accounts and permissions**.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click Next to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Copy Permissions from one share to another share(s)?

How to replace all explicit permissions existing in descendant with the inherited permissions from the target object?

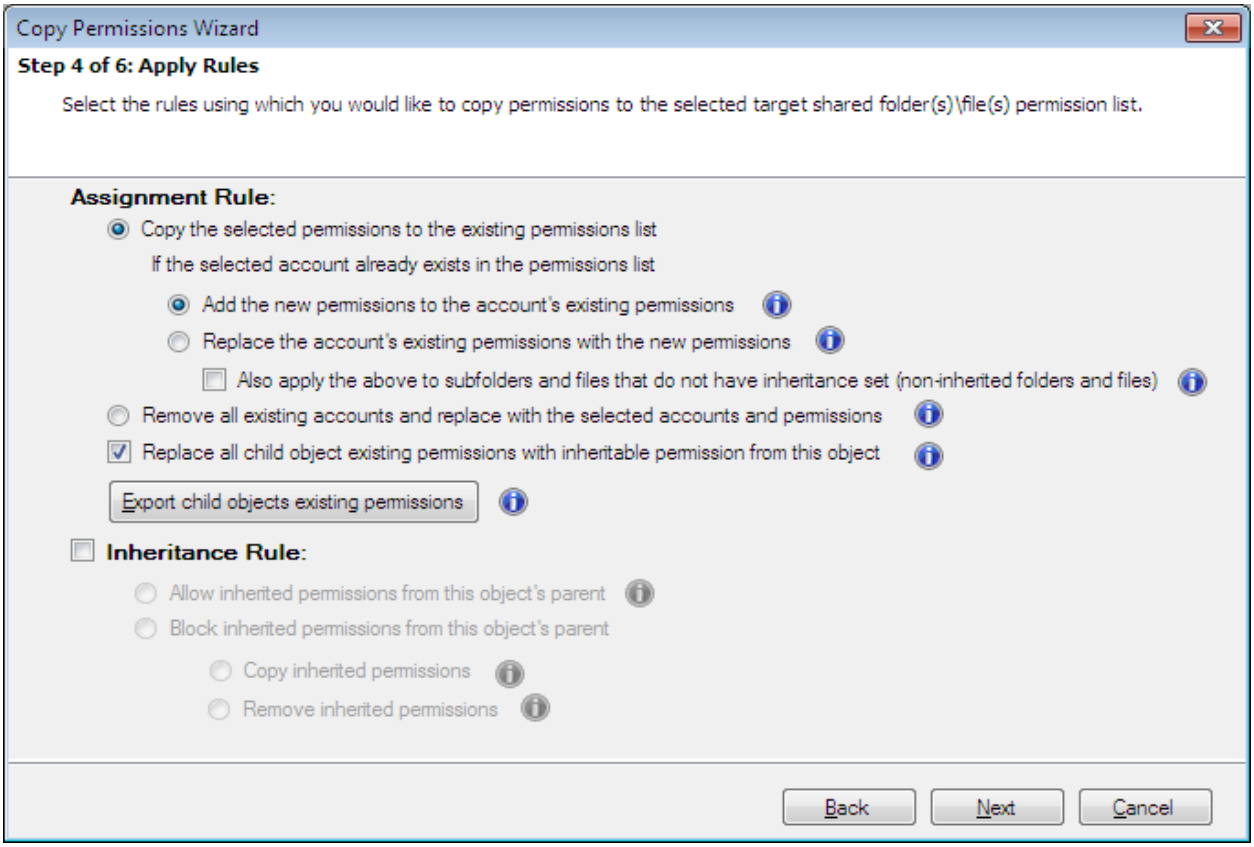
The **Copy Permissions** feature allows to remove explicitly defined permissions on all descendant object and replace them with the inheritable permissions from the target shared folder(s)/file(s) permissions list.

Click on 

button.

The Copy Permissions window will be displayed.

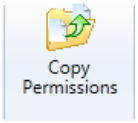
- Follow the steps 1 through 3 as outlined in How to Copy permissions from one share to another share(s)?
- In step 4 select the option **Replace all child objects existing permissions with the inheritable permissions from this object**.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Copy Permissions from one share to another Share(s)?

How to allow inherited permissions from the parent object to the target shares?

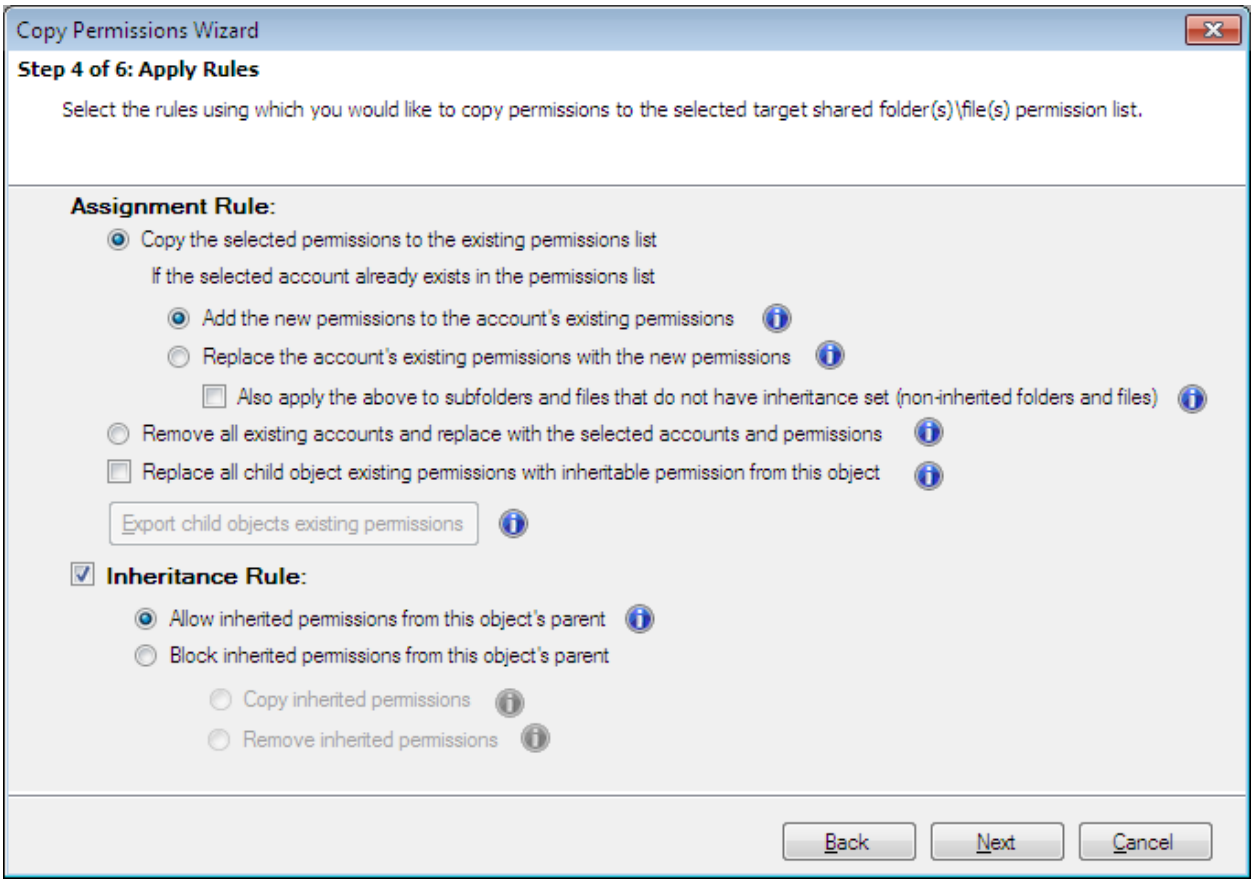
The **Copy Permissions** feature provides an option to Allow inheritable permissions from the parent object to the target shared folder(s)/file(s).

Click on 

button.

The Copy Permissions window will be displayed.

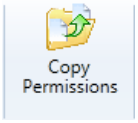
- Follow the steps 1 through 3 as outlined in How to Copy permissions from one share to another share(s)?
- In step 4 select the option **Inheritance Rule** and then select the option **Allow inherited permissions from this object's Parent**.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Copy permissions from one share to another share(s)?

How to block inherited permissions from the parent object to the target shares?

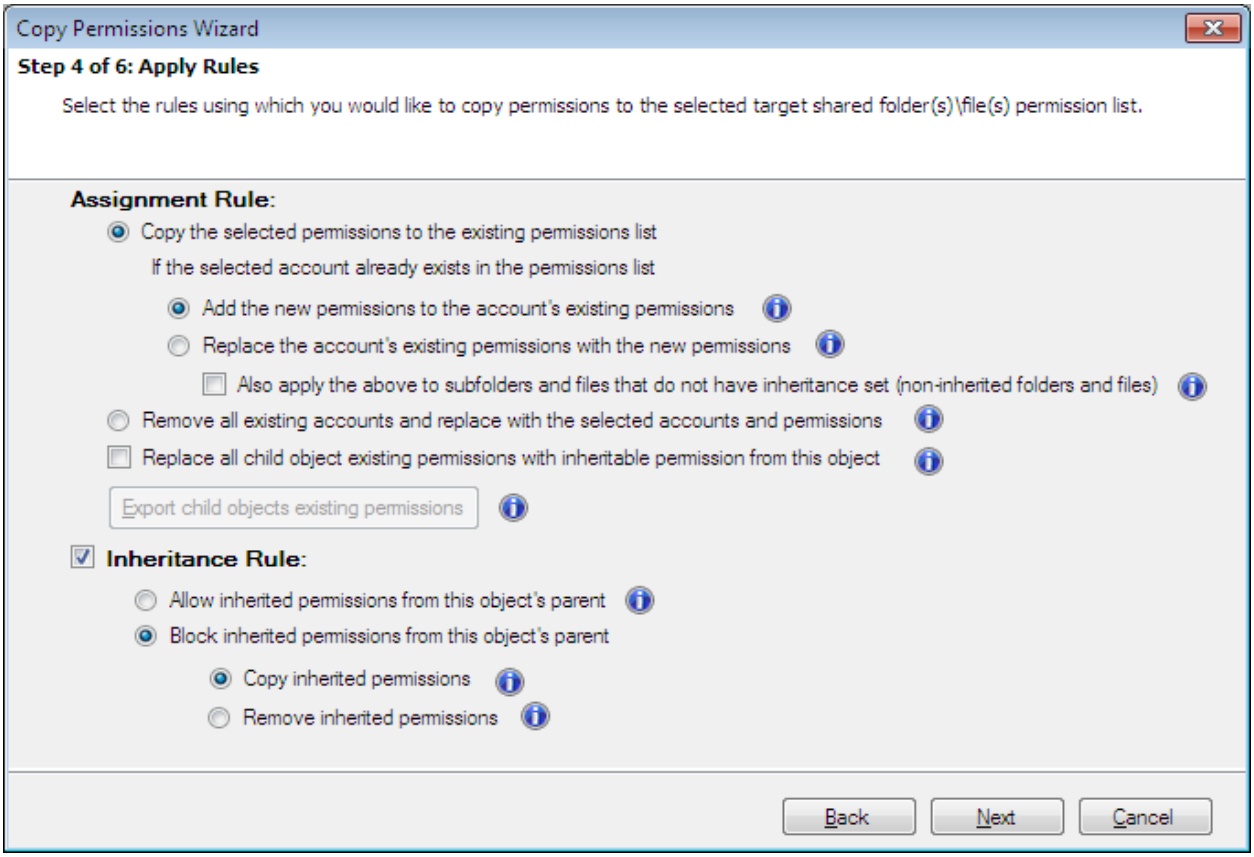
The **Copy Permissions** feature provides an option to Copy the inheritable permissions from the parent object to the target shares. This option will add the inherited permissions as explicit permissions in the target Shares permissions list. You can also remove the inherited permissions from the parent object to the target shares.

Click on 

button.

The Copy Permissions window will be displayed.

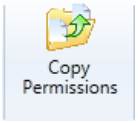
- Follow the steps 1 through 3 as outlined in How to Copy permissions from one share to another share(s)?
- In step 4 select the option Copy inherited permissions.
- If you wish to remove the inherited permissions from the target shares, you may use the option Remove inherited permissions to remove all the inherited permissions from the parent object.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

- Click **Next** to proceed to the next step.
- Follow the steps 5 through 6 as outlined in How to Copy permissions from one share to another share(s)?

How to Copy Permissions from one share to another share(s)?

The Copy Permissions feature allows you to Copy Permissions from one share to another share(s). You can use many options like Add the new permissions to the account's existing permissions, Replace the account's existing permissions with the new permissions, etc. You may select options to Allow, Block inheritance from the parent object and also Replace all child objects existing permissions with the inheritable permissions from this object while copying permissions for accounts.

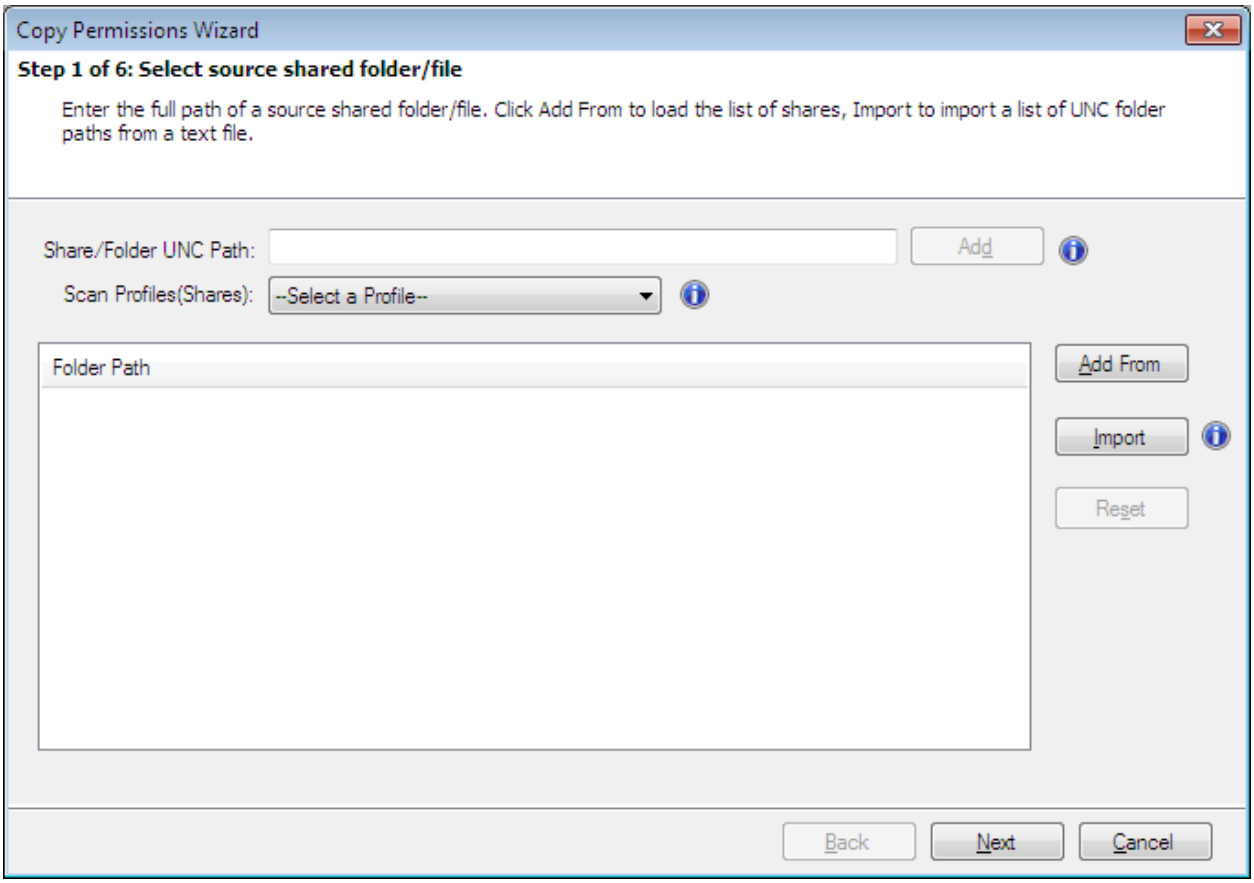
Click on 

button.

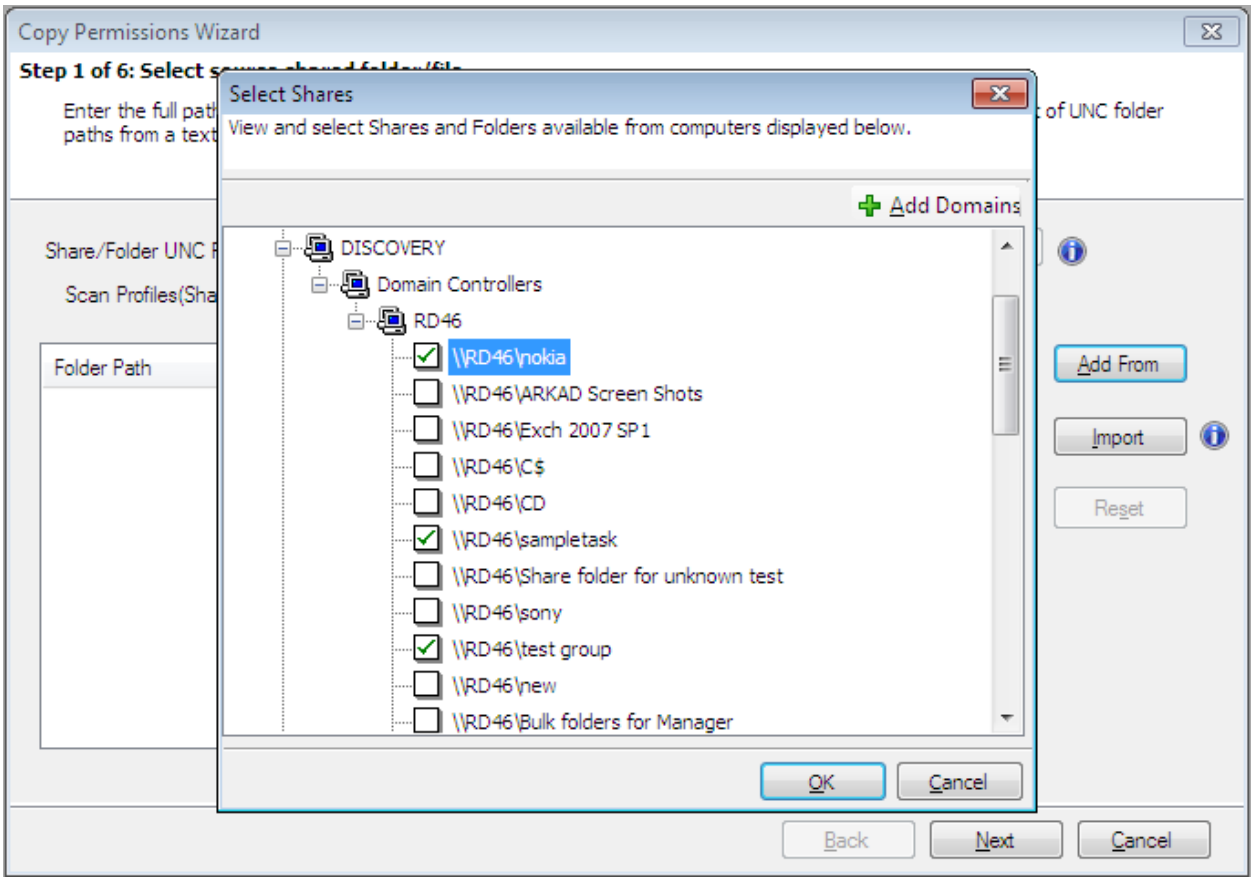
The Copy Permissions window will be displayed as shown below:

Step 1: Select source shared folder/file

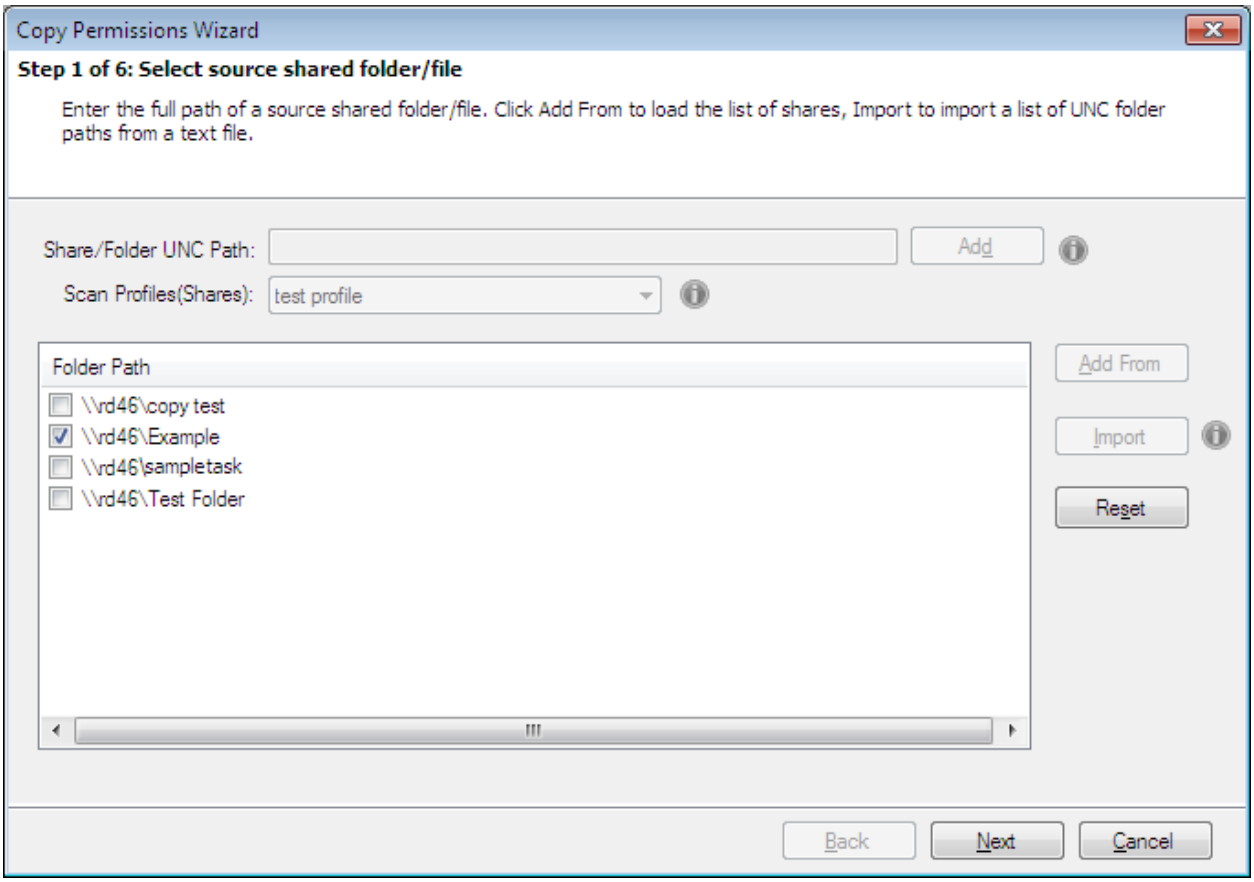
Select source shared folder/file by using any of the input options displayed.


Copy Permissions Wizard
Step 1 of 6: Select source shared folder/file
Enter the full path of a source shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profiles(Shares):
--Select a Profile--
Folder Path
Add From
Import
Reset
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click **Add From** option
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use **Select a Scan Profile (Shares)** option to use the shares added in the profile.

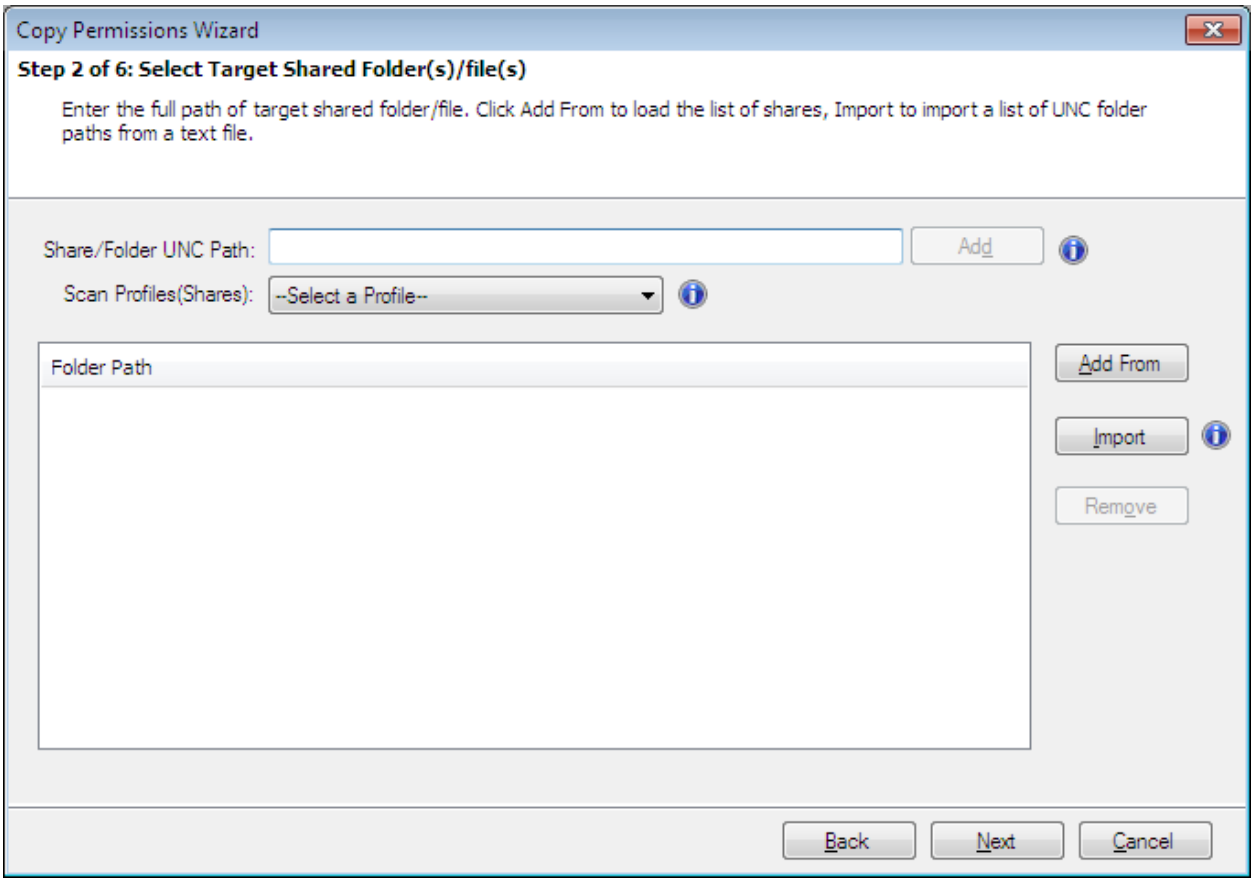


You may also type the UNC path of a shared folder that is not in the list and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared folder list from a text file by using the **Import** button.

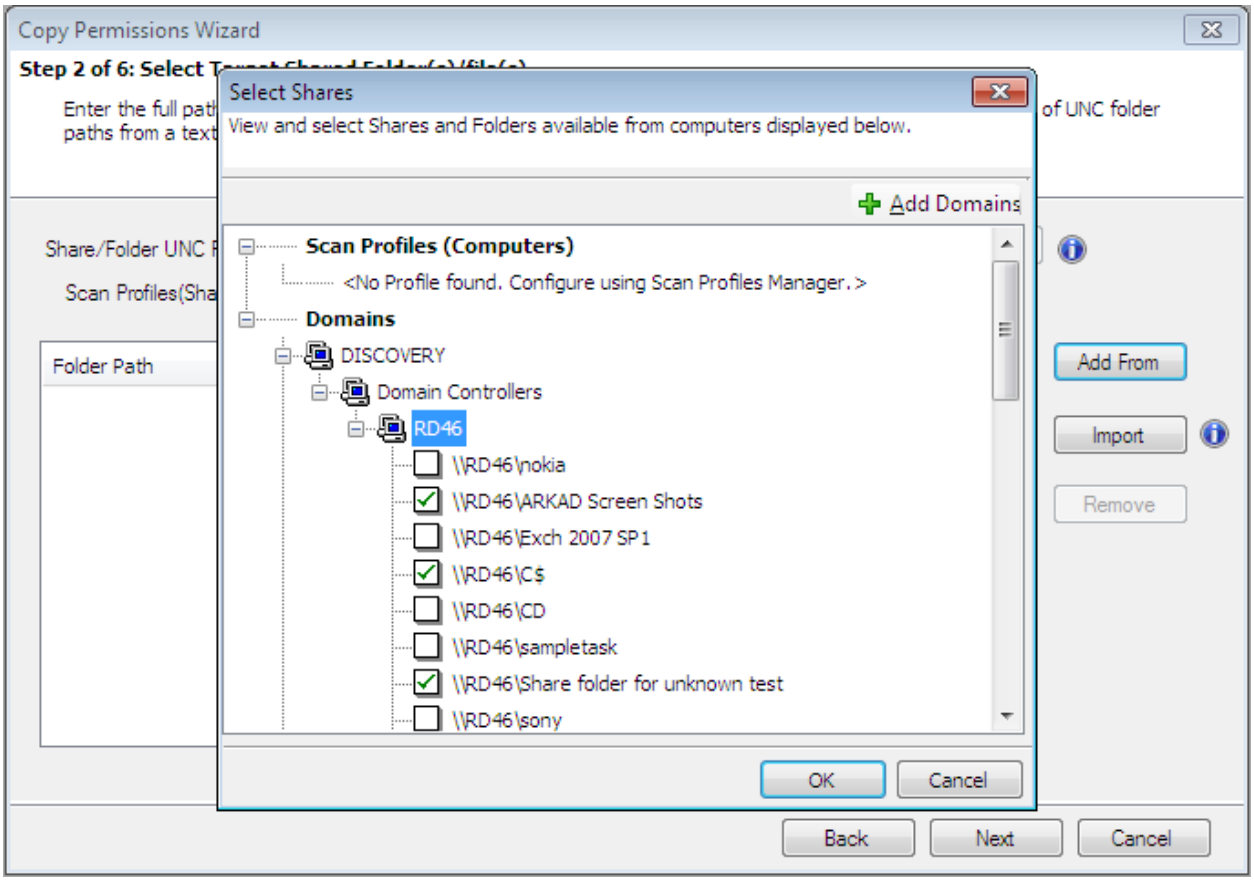
Click **Next** to proceed to the next step.

Step 2: Select target shared folder(s)/file(s)

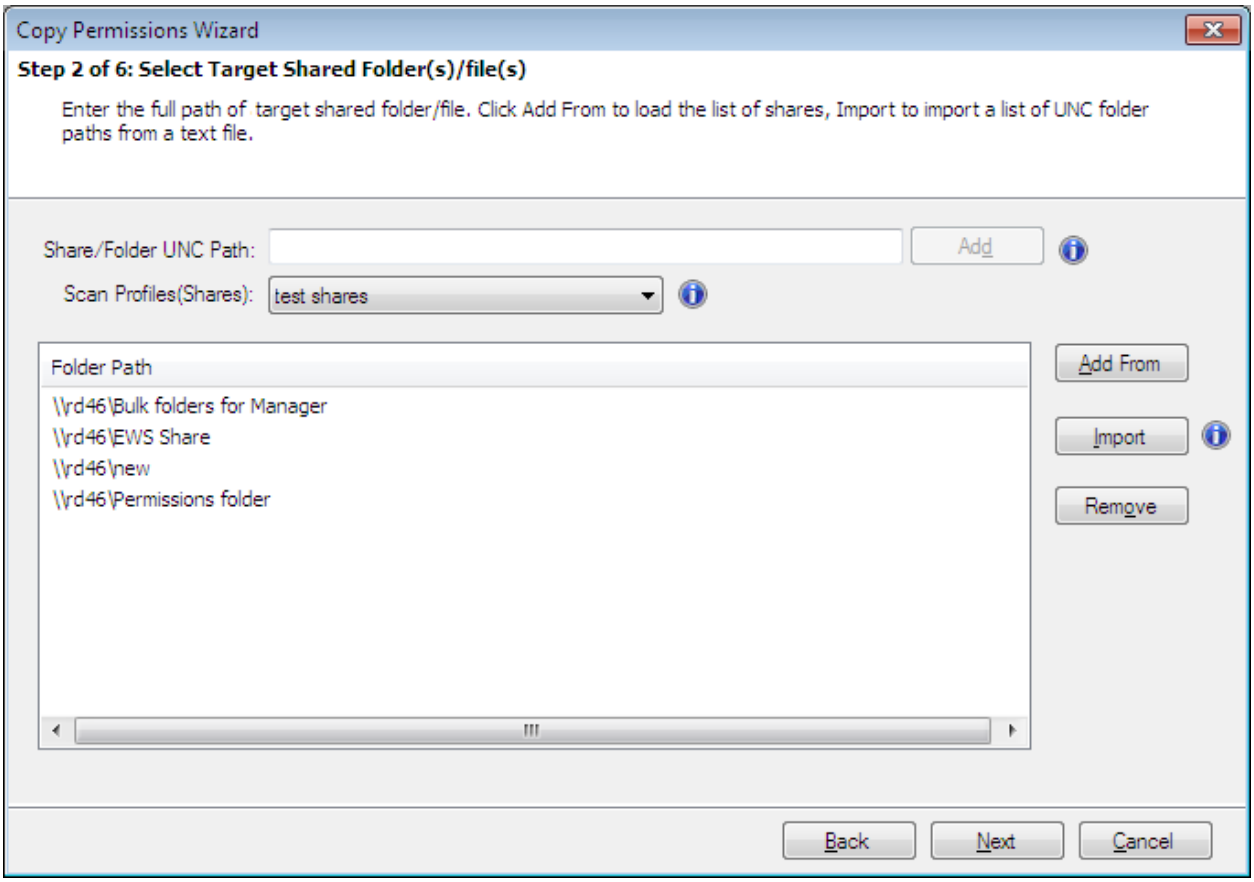
Select target shared folder(s)/file(s) by using any of the input options displayed


Copy Permissions Wizard
Step 2 of 6: Select Target Shared Folder(s)/file(s)
Enter the full path of target shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profiles(Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click **Add From** option
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use Select a **Scan Profile (Shares)** option to use the shares added in the profile.

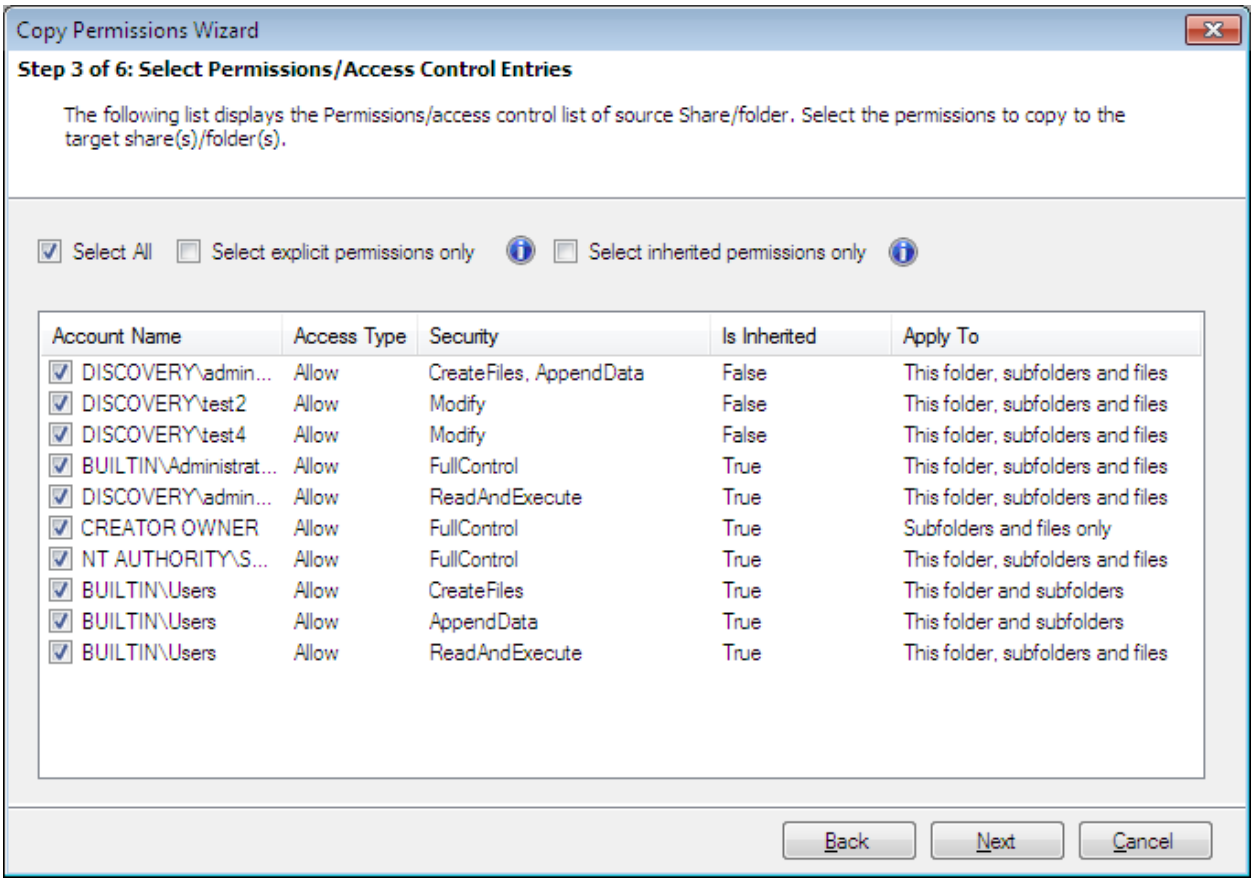


You may also type the UNC path of a shared folder that is not in the list and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared folder list from a text file by using the **Import** button.

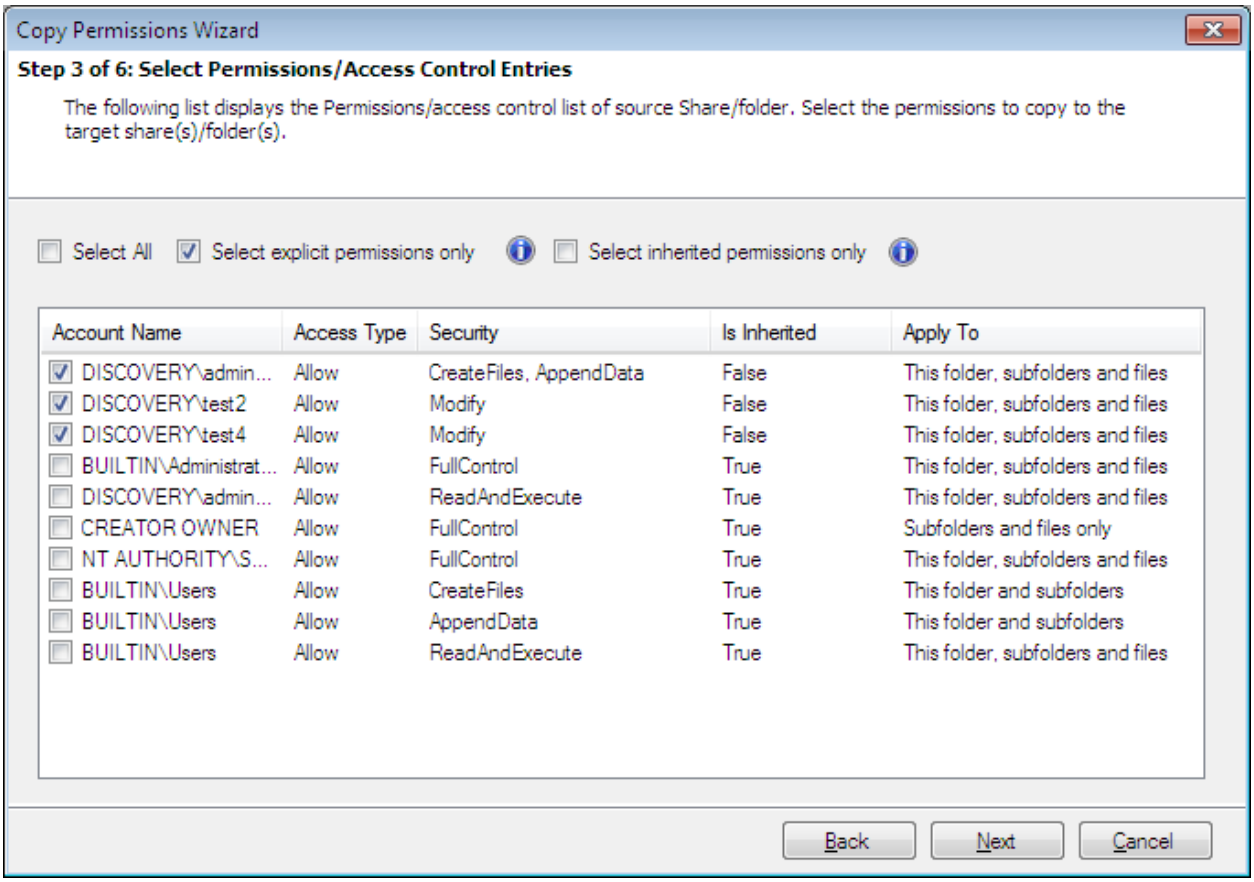
Click **Next** to proceed to the next step.

Step 3: Select Permissions/Access Control Entries

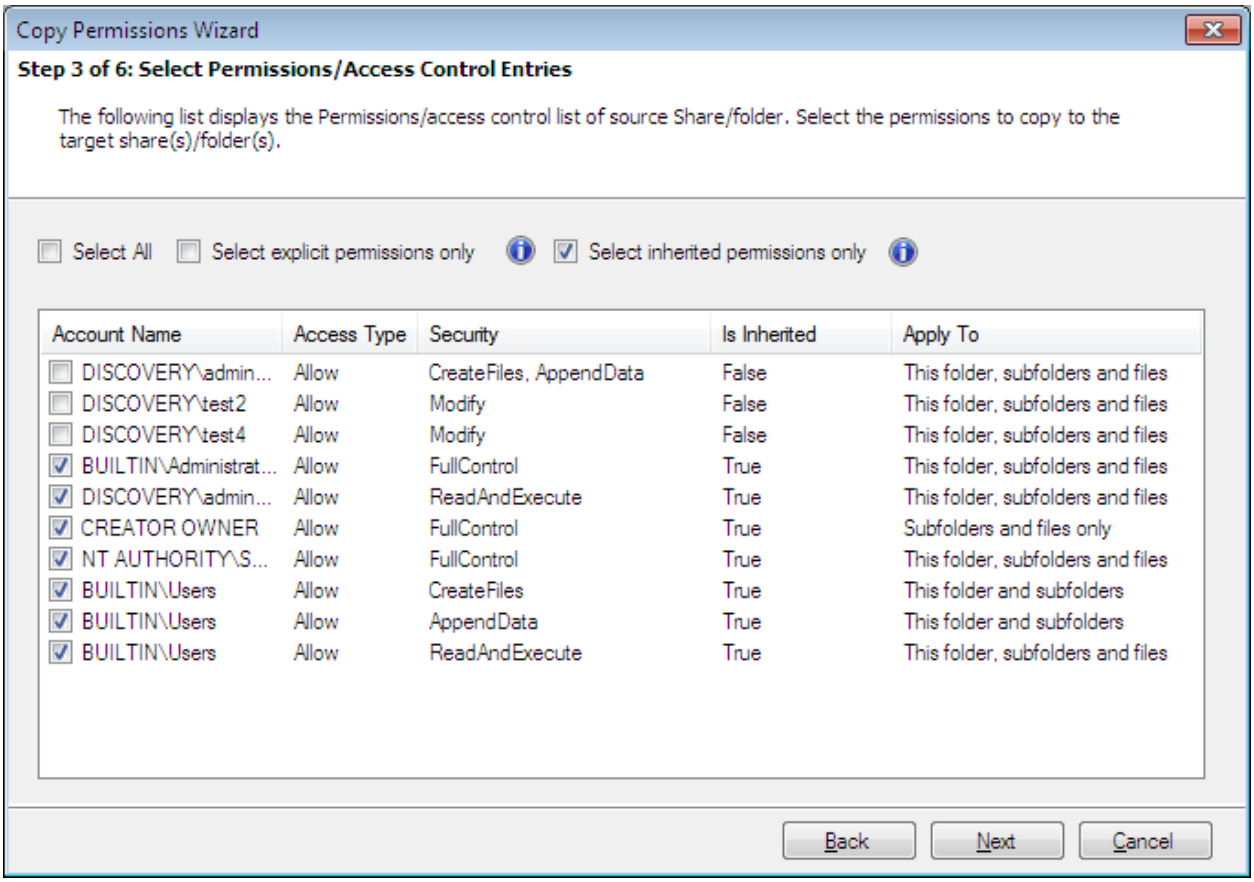
Select permissions/Access control entries to copy accounts to the selected target shared folder(s) /files(s)


Copy Permissions Wizard
Step 3 of 6: Select Permissions/Access Control Entries
The following list displays the Permissions/access control list of source Share/folder. Select the permissions to copy to the target share(s)/folder(s).
Select All
Select explicit permissions only
Select inherited permissions only
Account Name
Access Type
Security
Is Inherited
Apply To
DISCOVERY\admin... Allow CreateFiles, AppendData False This folder, subfolders and files
DISCOVERY\test2 Allow Modify False This folder, subfolders and files
DISCOVERY\test4 Allow Modify False This folder, subfolders and files
BUILTIN\Administrat... Allow FullControl True This folder, subfolders and files
DISCOVERY\admin... Allow ReadAndExecute True This folder, subfolders and files
CREATOR OWNER Allow FullControl True Subfolders and files only
NT AUTHORITY\S... Allow FullControl True This folder, subfolders and files
BUILTIN\Users Allow CreateFiles True This folder and subfolders
BUILTIN\Users Allow AppendData True This folder and subfolders
BUILTIN\Users Allow ReadAndExecute True This folder, subfolders and files
Back
Next
Cancel

- Use **Select explicit permissions only** option to select only explicit permissions from the source shared folder/file permissions list.


Copy Permissions Wizard
Step 3 of 6: Select Permissions/Access Control Entries
The following list displays the Permissions/access control list of source Share/folder. Select the permissions to copy to the target share(s)/folder(s).
Select All
Select explicit permissions only
Select inherited permissions only
Account Name
Access Type
Security
Is Inherited
Apply To
DISCOVERY\admin... Allow CreateFiles, AppendData False This folder, subfolders and files
DISCOVERY\test2 Allow Modify False This folder, subfolders and files
DISCOVERY\test4 Allow Modify False This folder, subfolders and files
BUILTIN\Administrat... Allow FullControl True This folder, subfolders and files
DISCOVERY\admin... Allow ReadAndExecute True This folder, subfolders and files
CREATOR OWNER Allow FullControl True Subfolders and files only
NT AUTHORITY\S... Allow FullControl True This folder, subfolders and files
BUILTIN\Users Allow CreateFiles True This folder and subfolders
BUILTIN\Users Allow AppendData True This folder and subfolders
BUILTIN\Users Allow ReadAndExecute True This folder, subfolders and files
Back
Next
Cancel

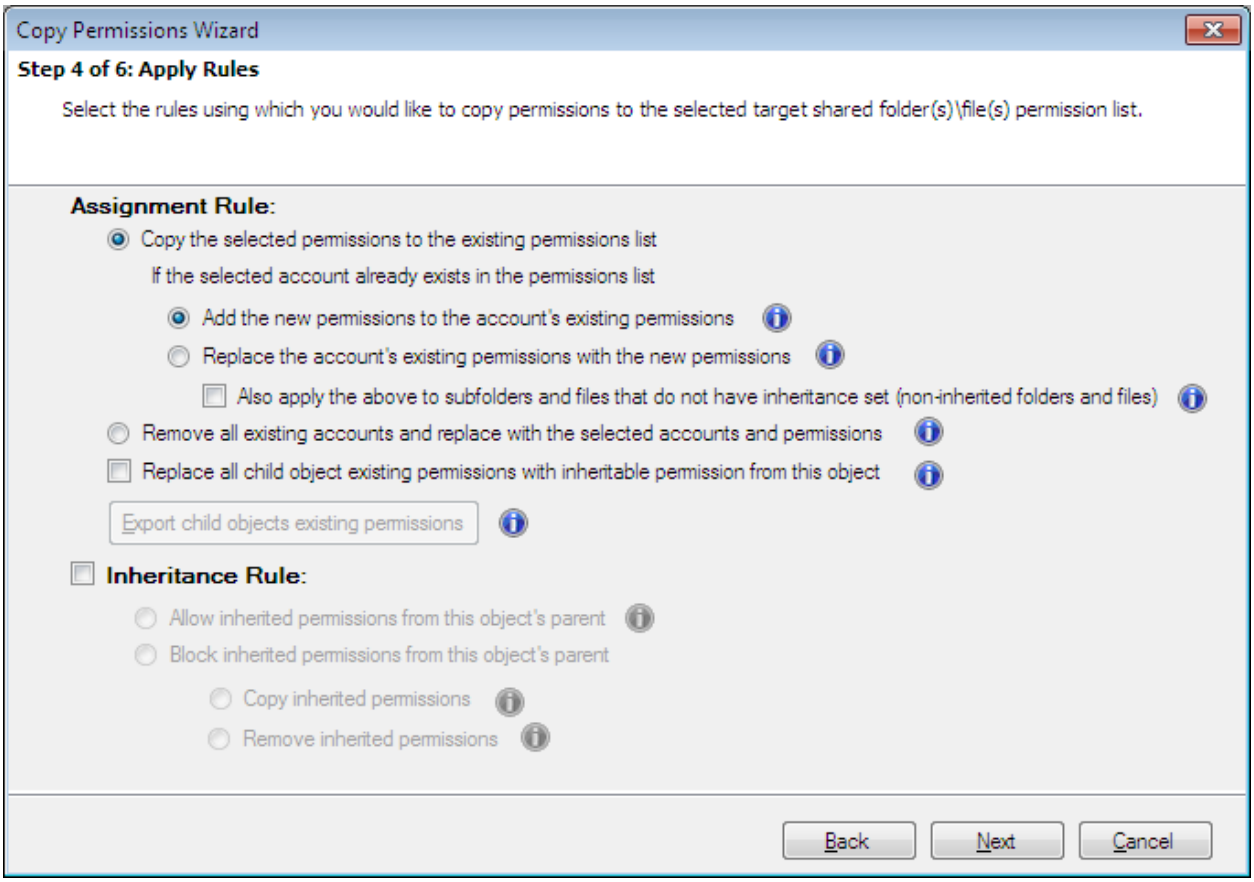
- Use **Select inherited permissions only** option to select only inherited permissions from the source shared folder/file permissions list.


Copy Permissions Wizard
Step 3 of 6: Select Permissions/Access Control Entries
The following list displays the Permissions/access control list of source Share/folder. Select the permissions to copy to the target share(s)/folder(s).
Select All
Select explicit permissions only
Select inherited permissions only
Account Name
Access Type
Security
Is Inherited
Apply To
DISCOVERY\admin... Allow CreateFiles, AppendData False This folder, subfolders and files
DISCOVERY\test2 Allow Modify False This folder, subfolders and files
DISCOVERY\test4 Allow Modify False This folder, subfolders and files
BUILTIN\Administrat... Allow FullControl True This folder, subfolders and files
DISCOVERY\admin... Allow ReadAndExecute True This folder, subfolders and files
CREATOR OWNER Allow FullControl True Subfolders and files only
NT AUTHORITY\S... Allow FullControl True This folder, subfolders and files
BUILTIN\Users Allow CreateFiles True This folder and subfolders
BUILTIN\Users Allow AppendData True This folder and subfolders
BUILTIN\Users Allow ReadAndExecute True This folder, subfolders and files
Back
Next
Cancel

Click Next to proceed to the next step.

Step 4: Apply the required rules to be used while copying permissions

Select which rules to apply while copying permissions.


Copy Permissions Wizard
Step 4 of 6: Apply Rules
Select the rules using which you would like to copy permissions to the selected target shared folder(s)\file(s) permission list.
Assignment Rule:
Copy the selected permissions to the existing permissions list
If the selected account already exists in the permissions list
Add the new permissions to the account's existing permissions
Replace the account's existing permissions with the new permissions
Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
Remove all existing accounts and replace with the selected accounts and permissions
Replace all child object existing permissions with inheritable permission from this object
Export child objects existing permissions
Inheritance Rule:
Allow inherited permissions from this object's parent
Block inherited permissions from this object's parent
Copy inherited permissions
Remove inherited permissions
Back
Next
Cancel

Add the new permissions to the account's existing permissions option will add the selected permissions to the existing permissions list and also it will not affect the existing permissions.

You may also use the below options to Copy Permissions and also apply inheritance by Inheritance rule.

- Replace the account's existing permissions with the new permissions.
- Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)
- Remove all existing accounts and replace with the selected accounts and permissions.
- Replace all child objects existing permissions with the inheritable permissions from this object.

Inheritance Rule:

- Allow inherited permissions from this object's parent.
- Copy inherited permissions.
- Remove inherited permissions.

Replace the account's existing permissions with the new permissions

If a selected account already exists in the current list of permissions of the selected target shared folder(s)/file(s), this option will replace all explicitly assigned account permissions with the newly selected permissions for that account.

Example: If the share already has some accounts with permissions like Allow Read and Write and if the same existing accounts selected with permissions Deny Modify to Copy Permissions then this option will replace the existing accounts previous permissions (Allow Read and Write) with new permission (Deny Modify). Otherwise if the selected account not exist in the share permissions list then it will add into the permissions list.

Also apply the above to subfolders and files that do not have inheritance set (non-inherited folders and files)

This option will copy permissions to the target object's subfolders and files that do not have inherited permissions from its parent object with respect to the above options.

Note: If this option is checked, the subfolders and files must have the applicable rights for the owner or the currently logged on user to perform this operation.

Example: If the target share has some subfolders and files with the blocked inheritance then this option will copy permissions based on the selected options.

Remove all existing accounts and replace with the selected accounts and permissions

This option will remove all existing accounts that have explicitly assigned permissions for the selected target shared folder(s)/file(s) and replace them with the selected accounts and permissions. Note that this will not remove inherited permissions from parent folder.

Caution: All existing account permissions will be cleaned up completely and the newly selected permissions will be applied.

Example: If the target share has 7 accounts then this option will remove all the 7 accounts and replace with the new selected accounts and permissions.

Replace all child objects existing permissions with the inheritable permissions from this object

This option will remove explicitly defined permissions on all descendants of the selected shared folder(s)/file(s) and replace them with inheritable permissions from the selected target shared folder(s)/file(s).

Example: If the target share has some subfolders with the explicitly assigned permissions and some subfolders with blocked inheritance then this option will remove all explicitly assigned permissions of subfolders and allow inherited permissions from the parent object.

Allow inherited permissions from this object's Parent

This option will allow the selected target shared folder(s)/file(s) to inherit permissions from its parent object.

Example: If the target share do not have any inherited permissions and the inheritance from the parent object blocked then this option will allow inherited permissions from the parent object.

Copy inherited permissions

This option will copy the permission entries that were previously inherited from the parent to this selected target shared folder(s)/file(s).

Example: If the target share already allowed to inherit permissions from parent object then this option will remove the inheritance and add the inherited permissions as explicit permissions in the permissions list.

Remove inherited permissions

This option will remove the permission entries that were previously inherited from the parent and keep only those permissions explicitly selected here.

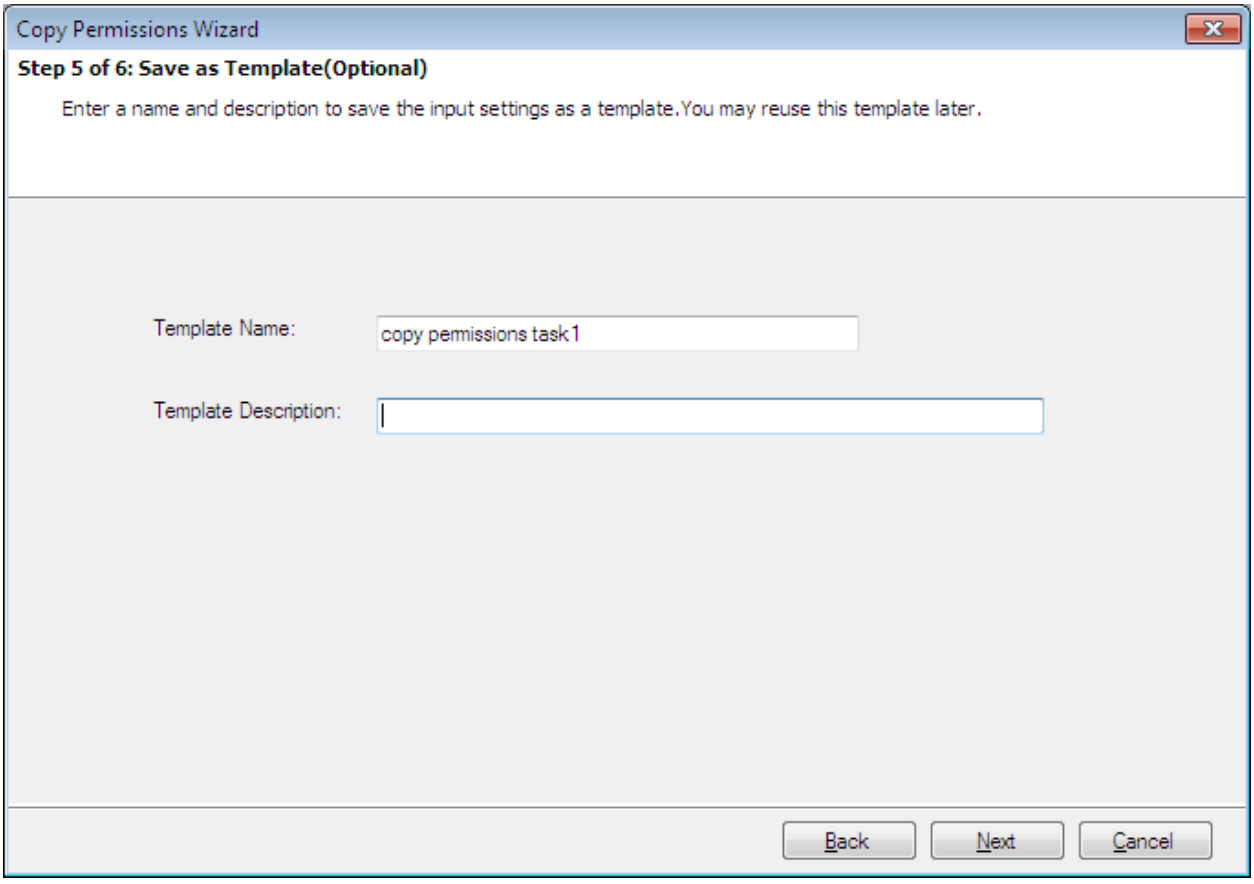
Caution: Removing permission inheritance from parent may break permissions/policies designed with the default inheritance option enabled. Use this option after a careful review.

Example: If the target share is already set to inherit permissions from parent object then this option will remove the inheritance from parent object.

Click **Next** to proceed to the Next step

Step 5: Save as template

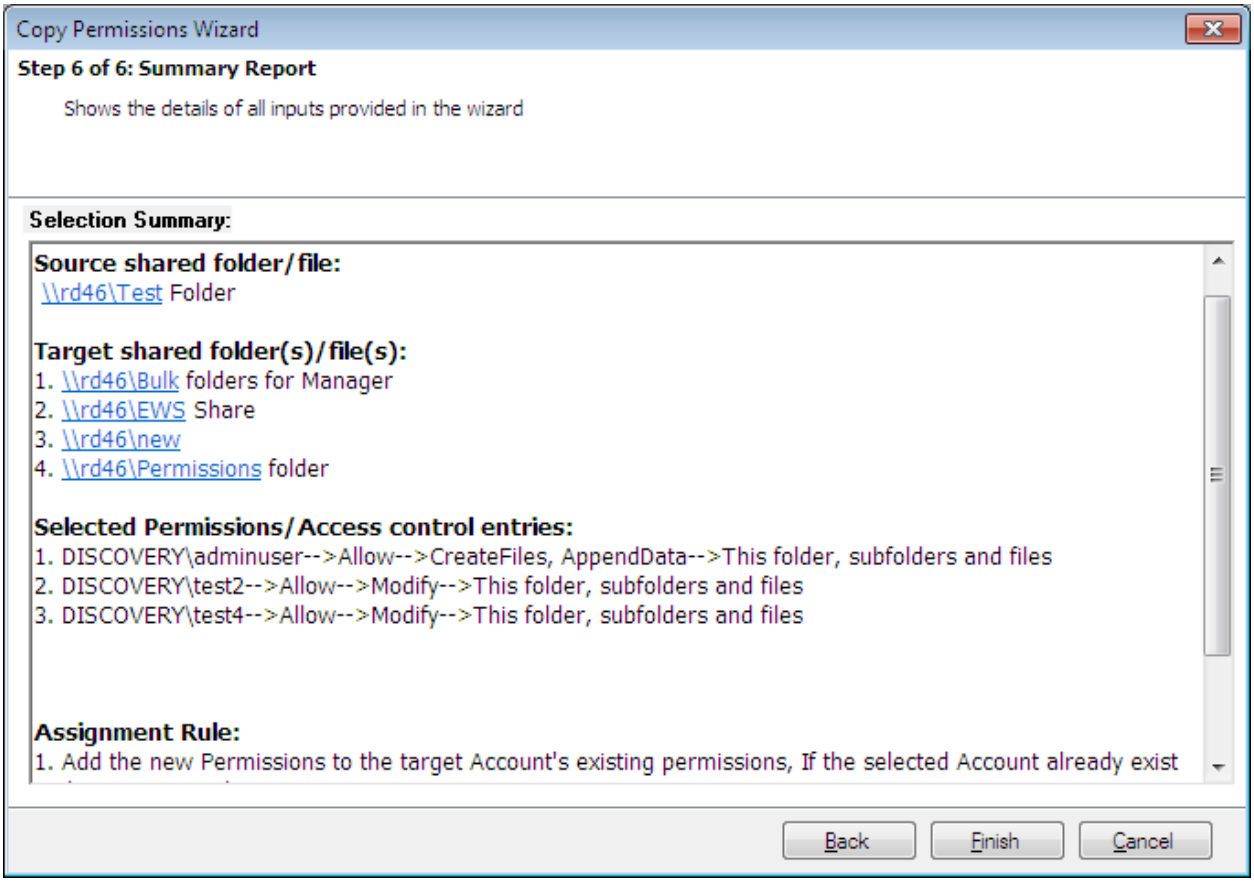
Enter a name and description to save the input settings as a template. You may reuse this template later.


Copy Permissions Wizard
Step 5 of 6: Save as Template(Optional)
Enter a name and description to save the input settings as a template.You may reuse this template later.
Template Name:
copy permissions task1
Template Description:
Back
Next
Cancel

Click **Next** to proceed to the next step

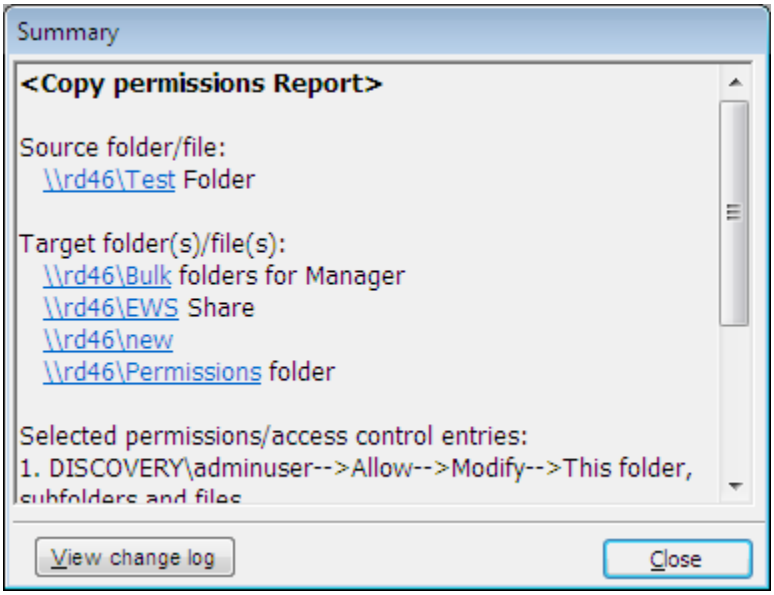
Step 6: Summary

This step displays the summary of all the input data along with the selected options.


Copy Permissions Wizard
Step 6 of 6: Summary Report
Shows the details of all inputs provided in the wizard
Selection Summary:
Source shared folder/file:
\\rd46\Test Folder
Target shared folder(s)/file(s):
1. \\rd46\Bulk folders for Manager
2. \\rd46\EWS Share
3. \\rd46\new
4. \\rd46\Permissions folder
Selected Permissions/Access control entries:
1. DISCOVERY\adminuser-->Allow-->CreateFiles, AppendData-->This folder, subfolders and files
2. DISCOVERY\test2-->Allow-->Modify-->This folder, subfolders and files
3. DISCOVERY\test4-->Allow-->Modify-->This folder, subfolders and files
Assignment Rule:
1. Add the new Permissions to the target Account's existing permissions, If the selected Account already exist
Back
Finish
Cancel

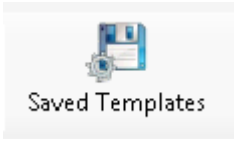
Click **Finish** to complete the Copy Permissions wizard.

Permissions will be copied as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.

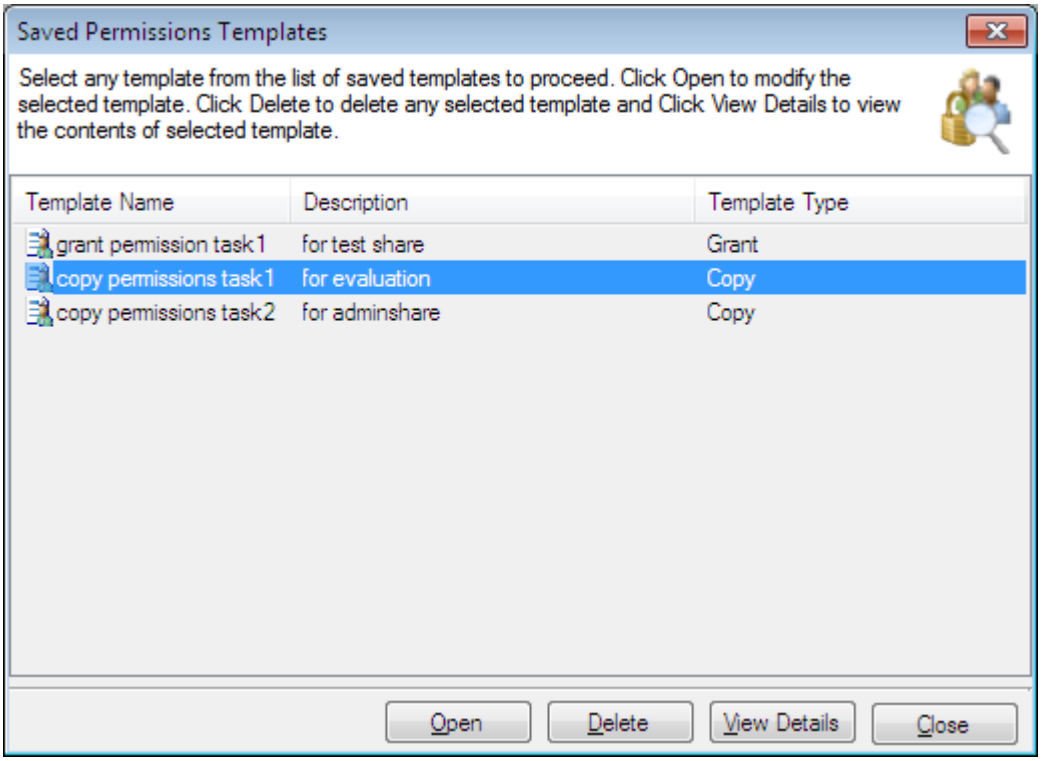

Summary
<Copy permissions Report>
Source folder/file:
\\rd46\Test Folder
Target folder(s)/file(s):
\\rd46\Bulk folders for Manager
\\rd46\EWS Share
\\rd46\new
\\rd46\Permissions folder
Selected permissions/access control entries:
1. DISCOVERY\adminuser-->Allow-->Modify-->This folder,
View change log
Close

How to reuse the Copy Permissions template?

The Saved Templates contains the list of saved templates to Grant, Revoke and Copy Permissions.

Click on 

button. The Saved Templates window will be displayed as shown below.



The saved templates window allows you to perform the following operations:

- Open an existing template
- Delete a template
- Preview the contents of a template

Open an existing Template

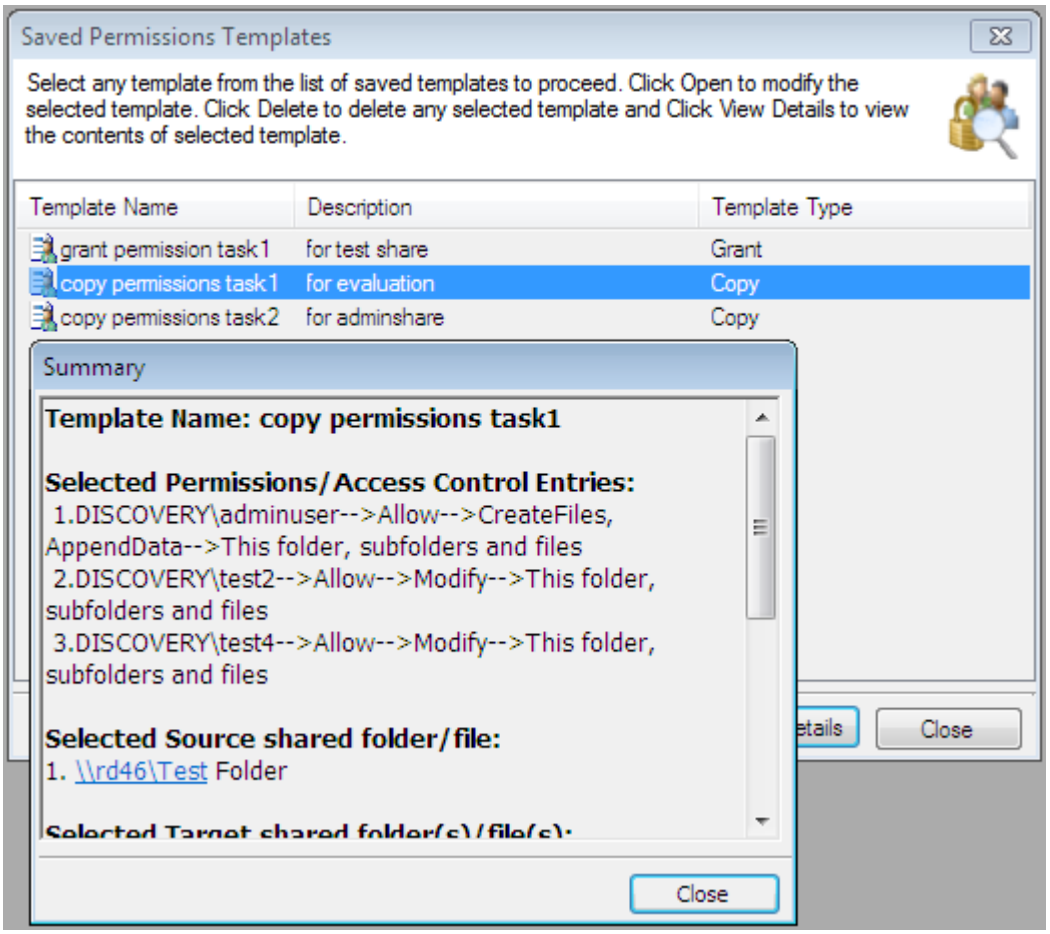
1. To open an existing Copy permissions template, select the Copy permissions template and click Open button in the window. The Copy permissions Dialog will appear on the screen which will allow you to edit the selected template.
2. During edit operation you can modify the computer list and permissions entries, however, you cannot modify the name of the template.

Delete a template

To delete a Copy permissions template, select a Copy permissions template which you want to delete, and then click Delete button. The selected template will be deleted permanently.

Preview the settings of a Template

To preview the settings of a saved Template, select a saved Copy permissions template, and then click View Details button. The settings will be displayed in a window as shown below:

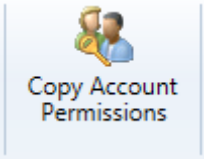

Saved Permissions Templates
Select any template from the list of saved templates to proceed. Click Open to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
grant permission task1
for test share
Grant
copy permissions task1
for evaluation
Copy
copy permissions task2
for adminshare
Copy
Summary
Template Name: copy permissions task1
Selected Permissions/Access Control Entries:
1.DISCOVERY\adminuser-->Allow-->CreateFiles, AppendData-->This folder, subfolders and files
2.DISCOVERY\test2-->Allow-->Modify-->This folder, subfolders and files
3.DISCOVERY\test4-->Allow-->Modify-->This folder, subfolders and files
Selected Source shared folder/file:
1. \\rd46\Test Folder
Close
Close

Copy Account Permissions

How to copy account permissions in the selected shared folder(s)/file(s) permissions list?

How to copy account permissions in the selected shared folder(s)/file(s) permissions list?

The Copy Account Permissions feature allows you to copy an existing account permissions to single or multiple accounts by granting the same existing permissions. You can copy account permissions on specified levels of sub-folder and also copy account permissions on sub-folders that match the specified search criteria.

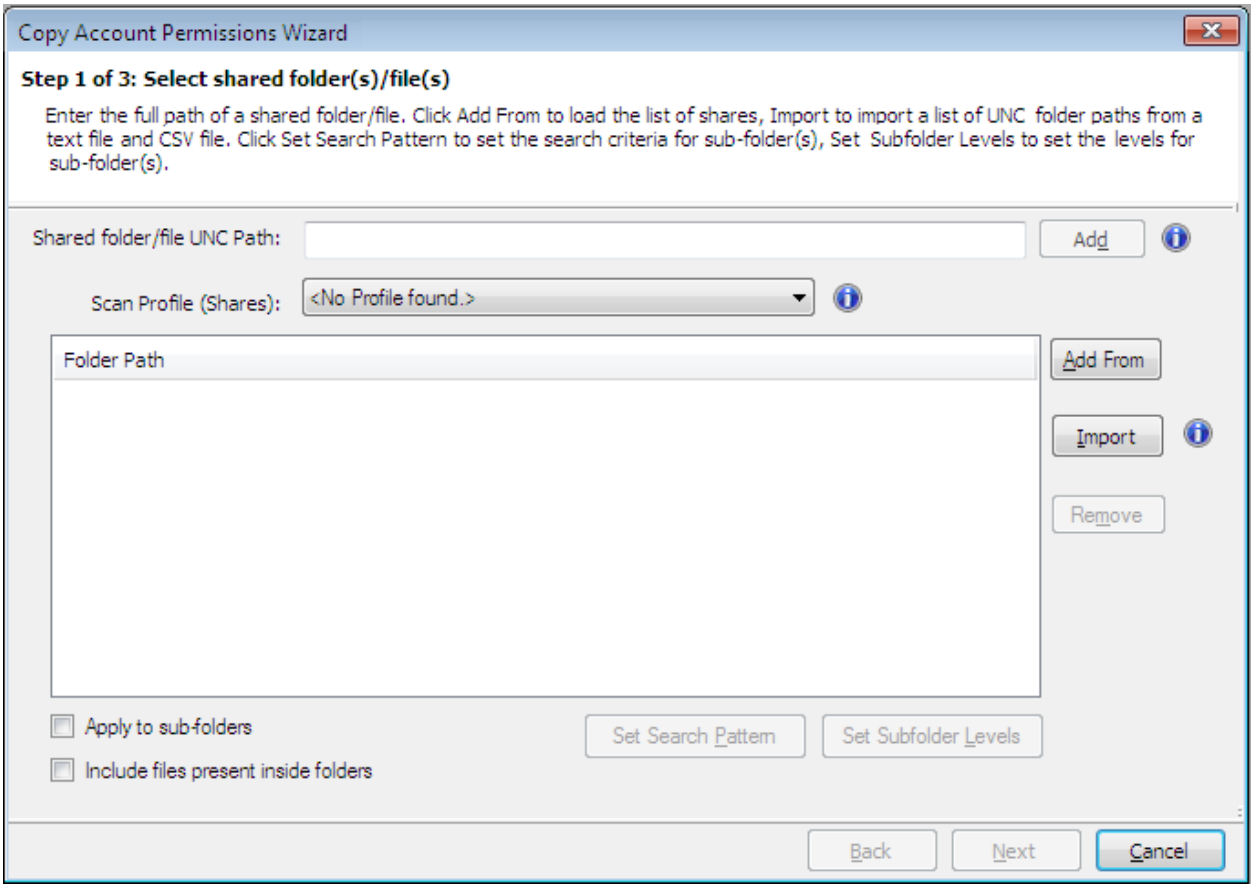
Click on 

button.

The Copy Account Permissions window will be displayed as shown below:

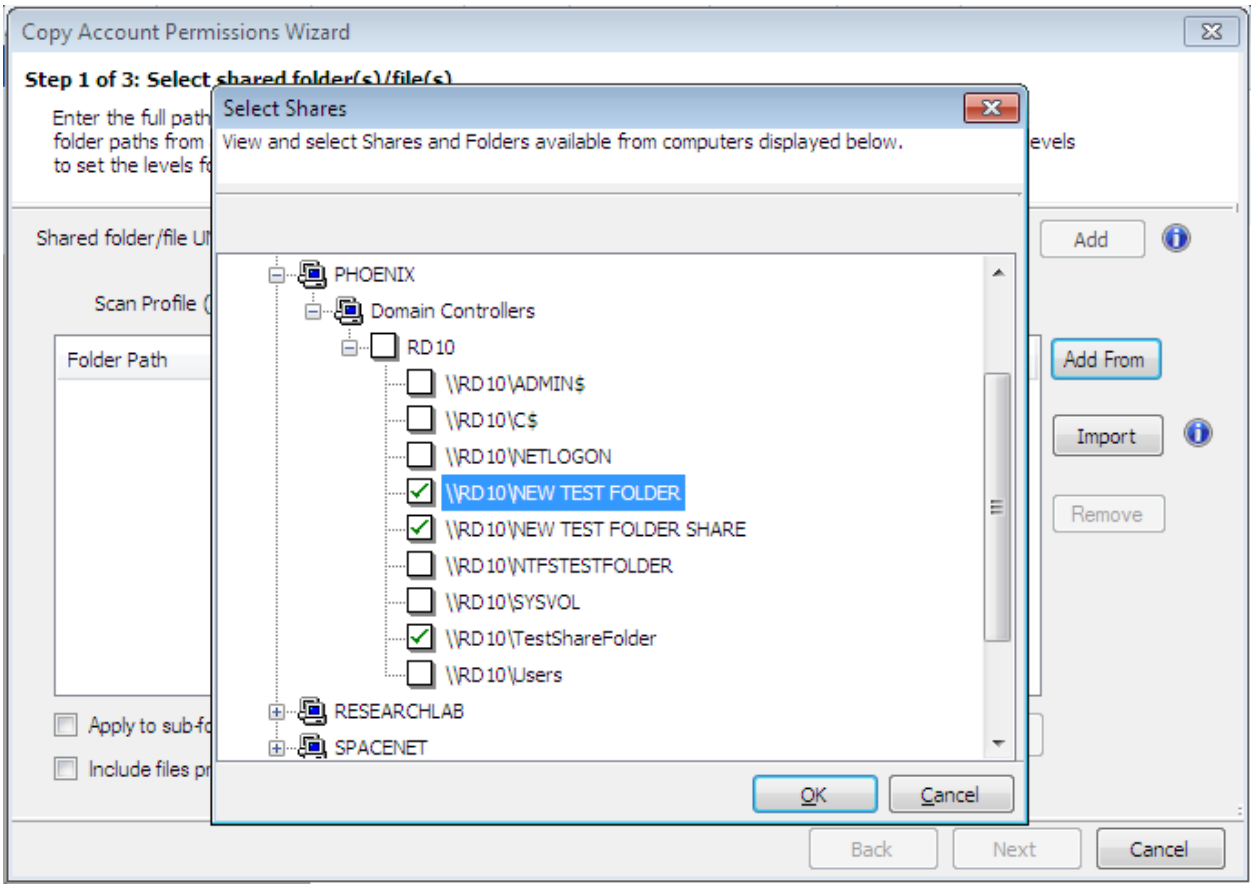
Step 1: Select shared folder(s)/file(s)

Select shared folder(s)/file(s) by using any of the input options displayed.

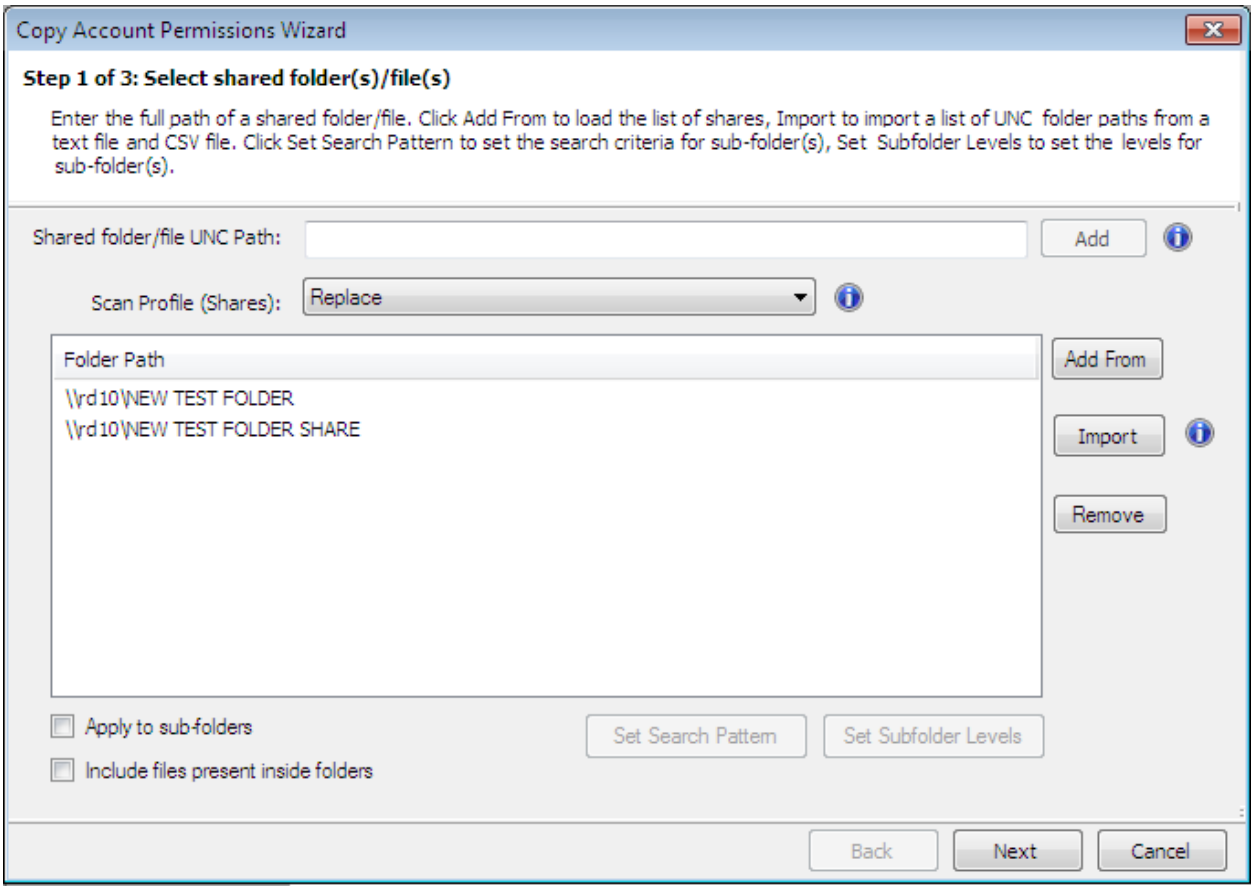

Copy Account Permissions Wizard
Step 1 of 3: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Click Set Search Pattern to set the search criteria for sub-folder(s), Set Subfolder Levels to set the levels for sub-folder(s).
Shared folder/file UNC Path:
Add
Scan Profile (Shares):
<No Profile found.>
Folder Path
Add From
Import
Remove
Apply to sub-folders
Include files present inside folders
Set Search Pattern
Set Subfolder Levels
Back
Next
Cancel

If you want to select shares from servers for which you wish to add, then click Add From option

Select one or more servers to enumerate its shared folder(s)/file(s)



Use Select a Scan Profile (Shares) option to use the Shares added in the profile.

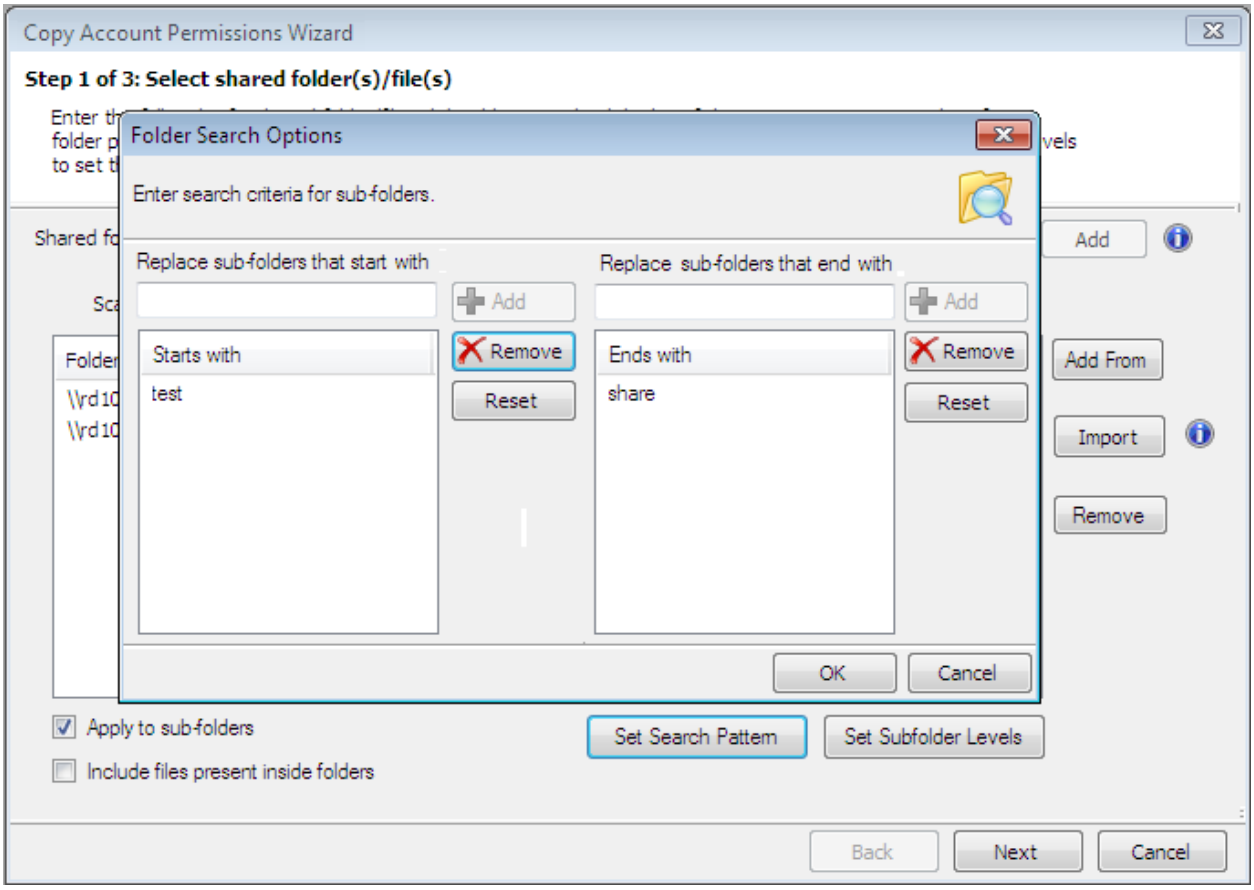

Copy Account Permissions Wizard
Step 1 of 3: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Click Set Search Pattern to set the search criteria for sub-folder(s), Set Subfolder Levels to set the levels for sub-folder(s).
Shared folder/file UNC Path:
Add
Scan Profile (Shares):
Replace
Folder Path
\\rd10\NEW TEST FOLDER
\\rd10\NEW TEST FOLDER SHARE
Add From
Import
Remove
Apply to sub-folders
Include files present inside folders
Set Search Pattern
Set Subfolder Levels
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file and CSV file by using the Import button.

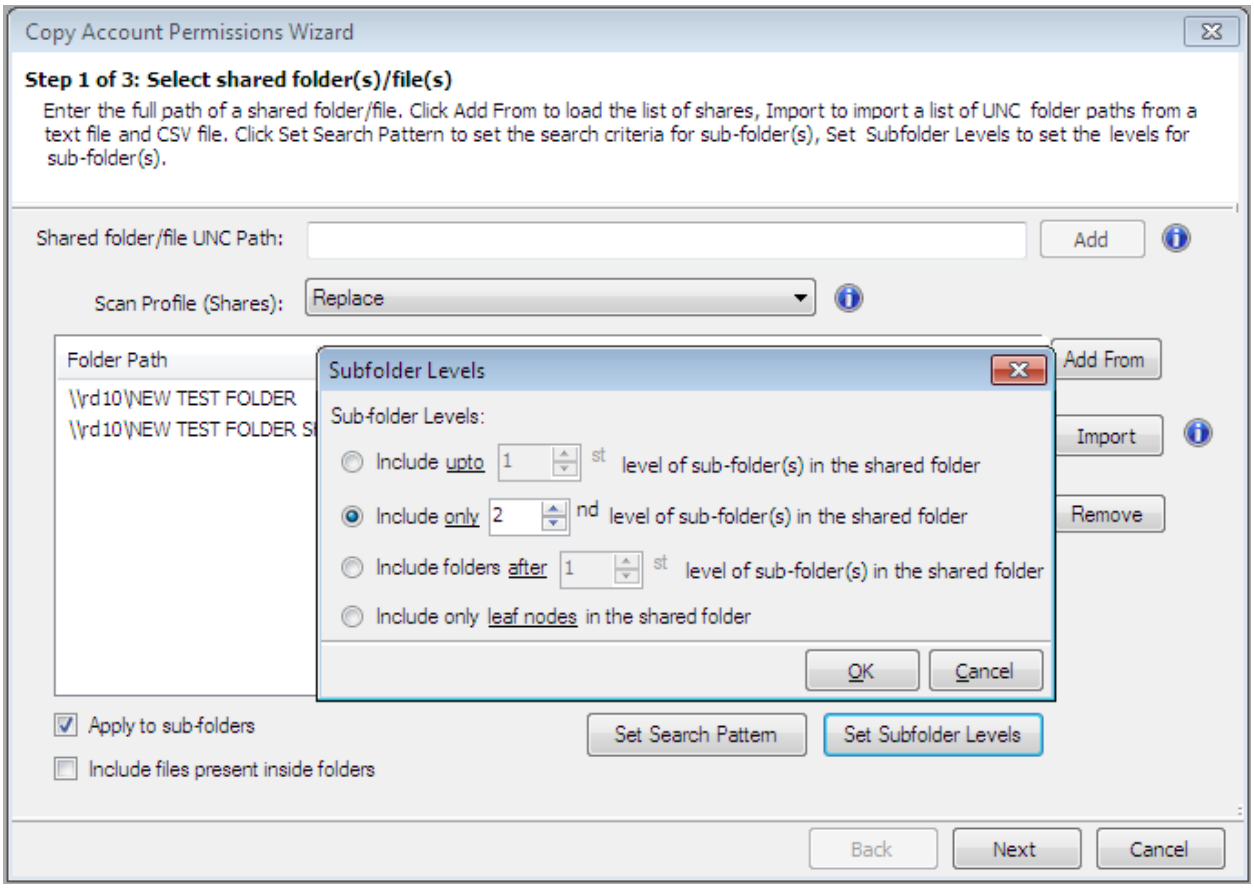
Apply to sub-folders: This option will copy an account permissions on sub-folders of the selected folders.

Include files present inside folders: This option will copy an account permissions on files present inside the selected folders.

Use Set Search Pattern option to copy an account permissions for sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example: Folder name starts with test, Folder name ends with share.



Use Set Subfolder Levels option to copy an account permissions in the selected levels of sub-folder(s) in the shared folder.


Copy Account Permissions Wizard
Step 1 of 3: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Click Set Search Pattern to set the search criteria for sub-folder(s), Set Subfolder Levels to set the levels for sub-folder(s).
Shared folder/file UNC Path:
Add
Scan Profile (Shares):
Replace
Folder Path
\\rd10\NEW TEST FOLDER
\\rd10\NEW TEST FOLDER S
Add From
Import
Remove
Subfolder Levels
Sub-folder Levels:
Include upto 1 st level of sub-folder(s) in the shared folder
Include only 2 nd level of sub-folder(s) in the shared folder
Include folders after 1 st level of sub-folder(s) in the shared folder
Include only leaf nodes in the shared folder
OK
Cancel
Apply to sub-folders
Include files present inside folders
Set Search Pattern
Set Subfolder Levels
Back
Next
Cancel

Include upto N level(s) of sub-folder(s) in the shared folder: This option will copy an account permissions on sub-folders which are upto the specified folder traversal level.

Include only Nth level of sub-folder(s) in the shared folder: This option will copy an account permissions on sub-folders which are in the specified folder level only.

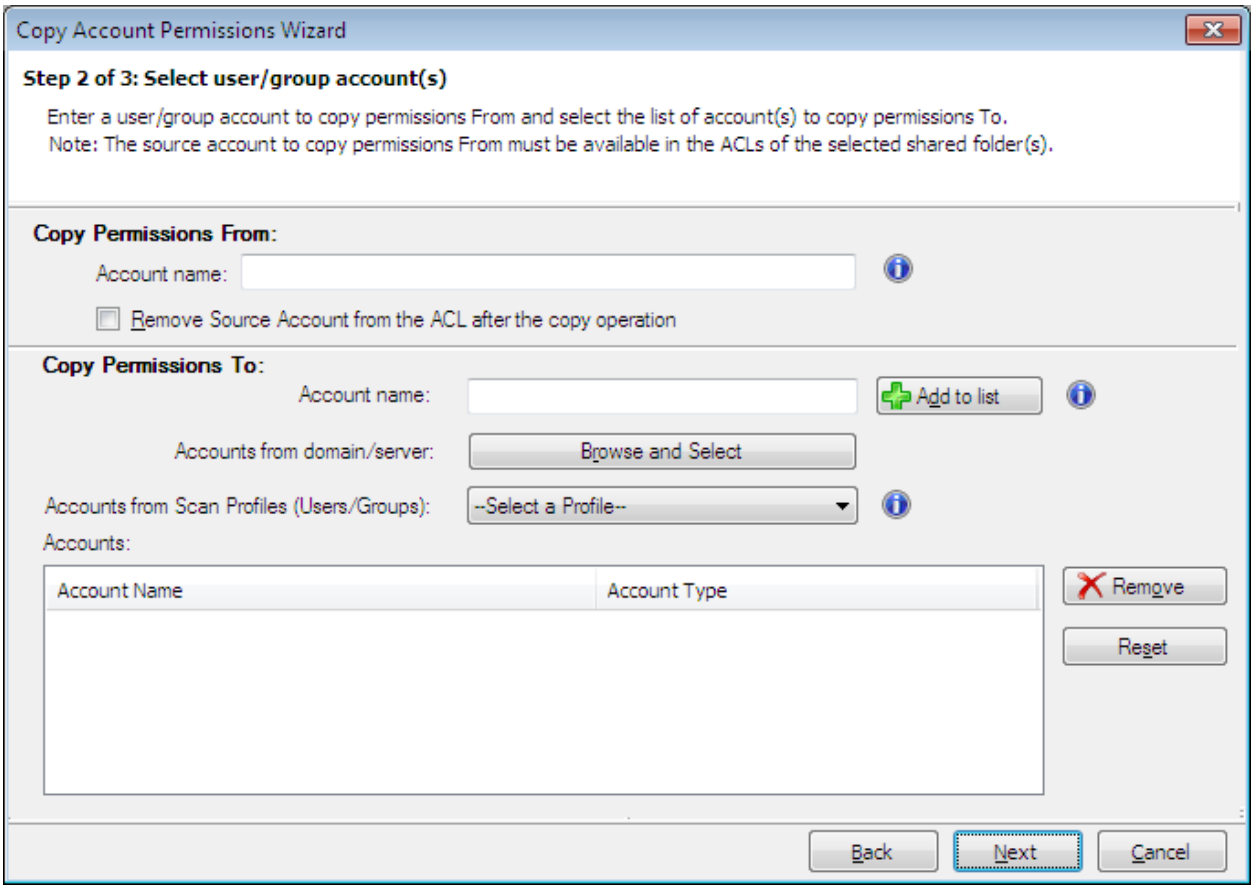
Include folders after N level(s) of sub-folder(s) in the shared folder: This option will copy an account permissions on sub-folders which are after the nth folder level of the selected folder.

Include only leaf nodes in the shared folder: This option will copy an account permissions on the last child (leaf) nodes without affecting the parent folder's permissions.

Click Next to proceed to the Next step.

Step 2: Select user/group account(s)

The User/Group Account(s) will be added to the wizard as shown below

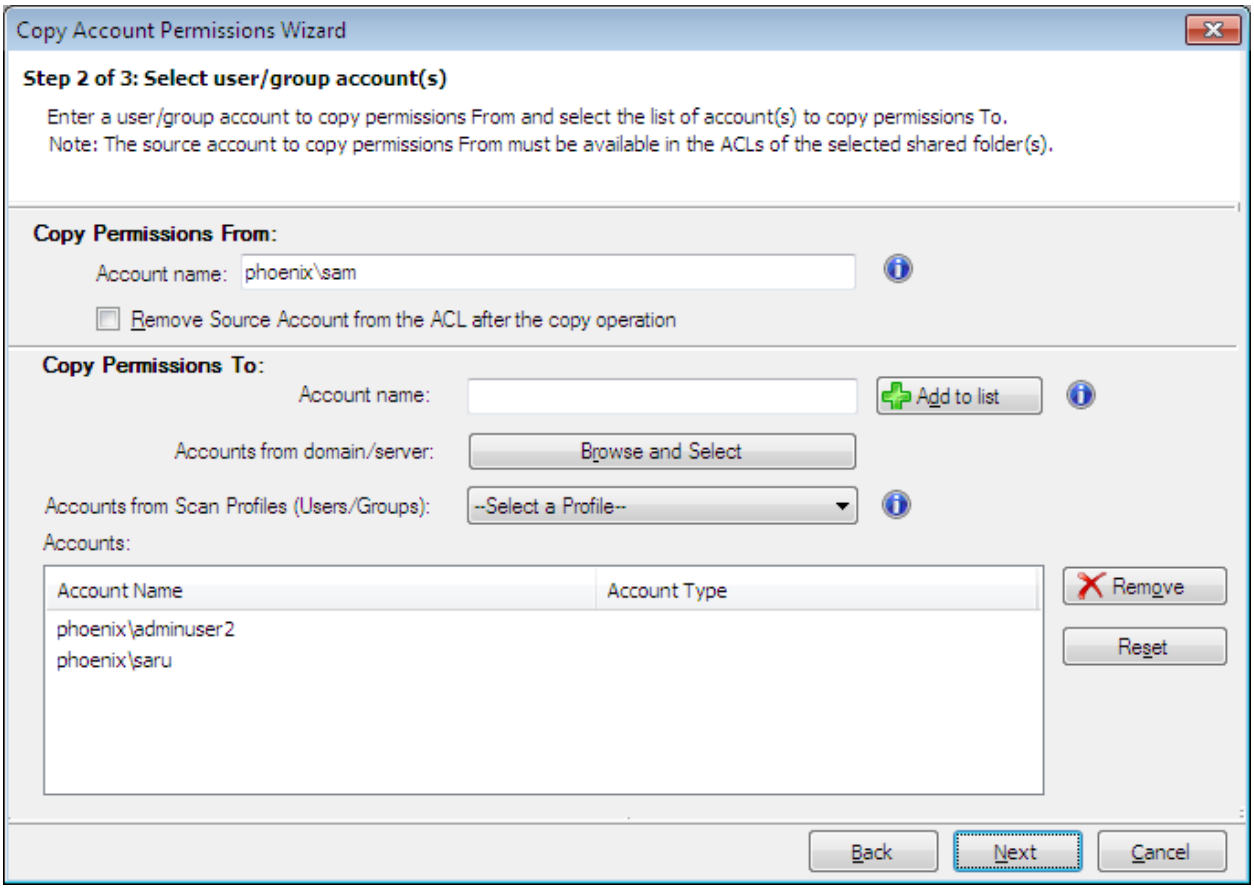

Copy Account Permissions Wizard
Step 2 of 3: Select user/group account(s)
Enter a user/group account to copy permissions From and select the list of account(s) to copy permissions To.
Note: The source account to copy permissions From must be available in the ACLs of the selected shared folder(s).
Copy Permissions From:
Account name:
Remove Source Account from the ACL after the copy operation
Copy Permissions To:
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
--Select a Profile--
Accounts:
Account Name
Account Type
Remove
Reset
Back
Next
Cancel

Enter a user or group account, for which you wish to Copy Permissions From.

Note: The source account to copy permissions From must be available in the ACLs of the selected shared folder(s).

Use Remove Source Account from the ACL after the copy operation option to remove the source account from the ACL once the copy operation is complete.

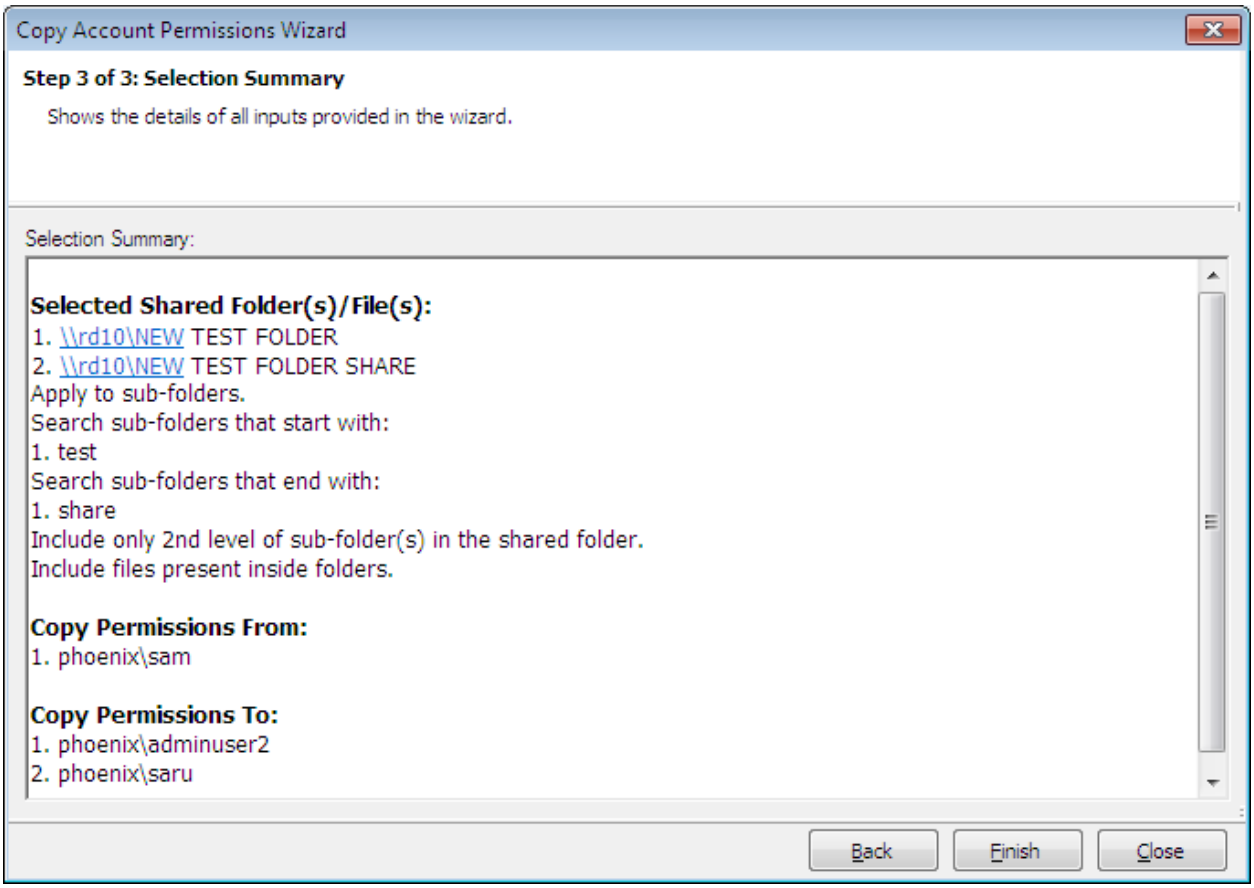
Select the list of user or group accounts, for which you wish to Copy Permissions To.


Copy Account Permissions Wizard
Step 2 of 3: Select user/group account(s)
Enter a user/group account to copy permissions From and select the list of account(s) to copy permissions To.
Note: The source account to copy permissions From must be available in the ACLs of the selected shared folder(s).
Copy Permissions From:
Account name: phoenix\sam
Remove Source Account from the ACL after the copy operation
Copy Permissions To:
Account name:
Add to list
Accounts from domain/server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
--Select a Profile--
Accounts:
Account Name
Account Type
phoenix\adminuser2
phoenix\saru
Remove
Reset
Back
Next
Cancel

Click Next to proceed to the next step.

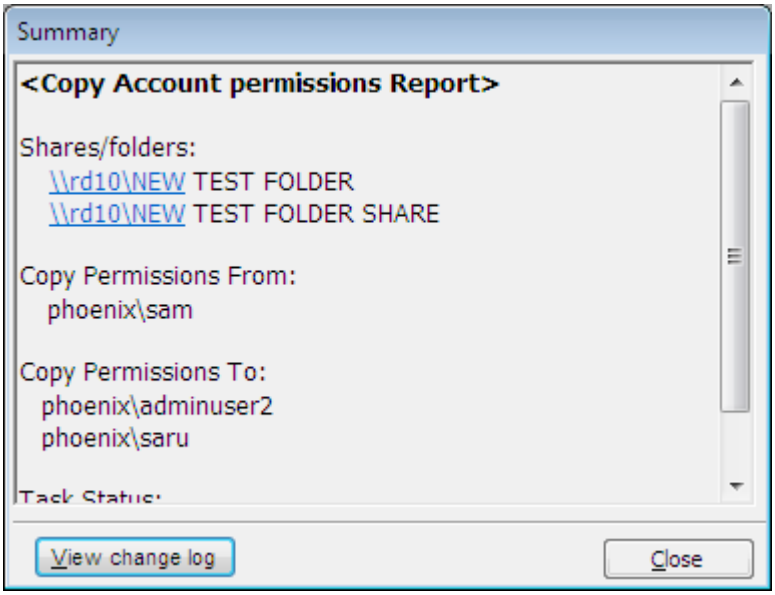
Step 3: Selection Summary

This step displays the summary of data selected to copy account permissions.



Click **Finish** to complete the Copy Account permissions wizard.

Permissions will be copied as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.



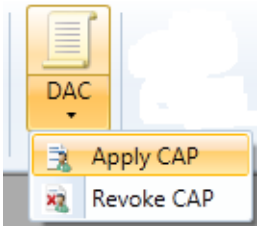
Dynamic Access Control

Apply Central Access Policy

Revoke Central Access Policy

How to Apply Central Access Policy on selected Shares?

The **Apply CAP** feature allows you to apply central access policy on the selected shared folder(s)/file(s). You can view and select the required Central Access Policy from the domain that belongs to the selected shared folder(s)/file(s).

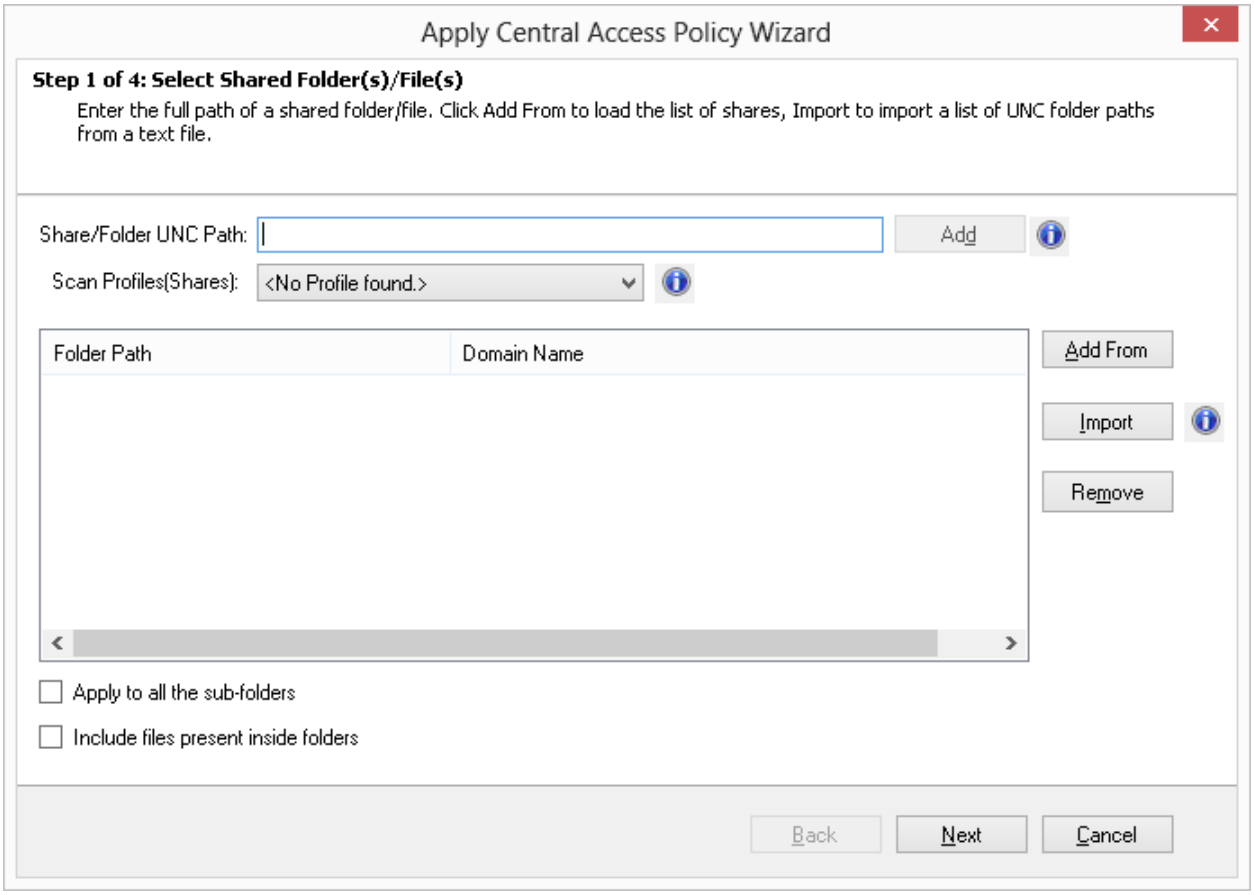
Click on 

button in the toolbar.

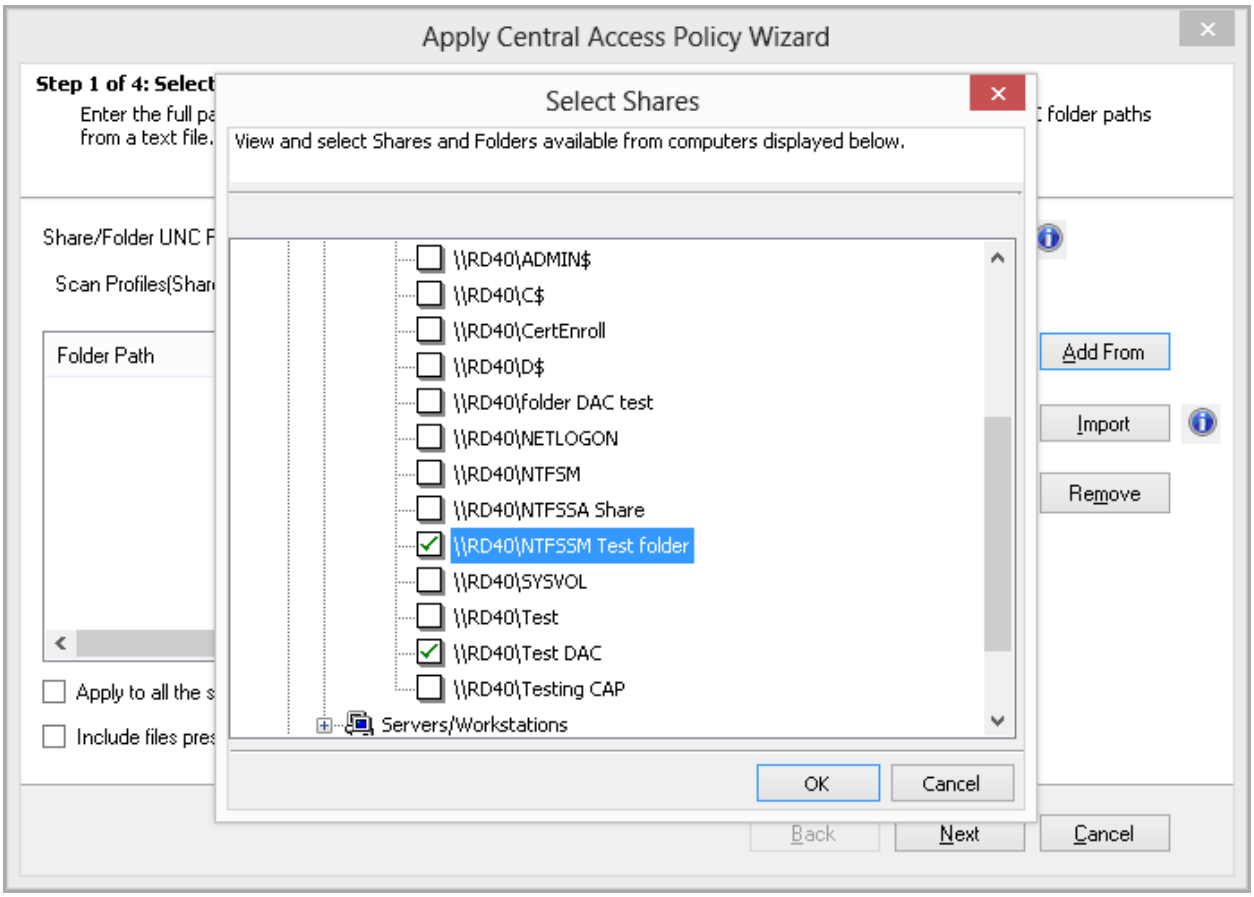
The Apply Central Access Policy window will be displayed as shown below:

Step 1: Select shared folder(s)/file(s)

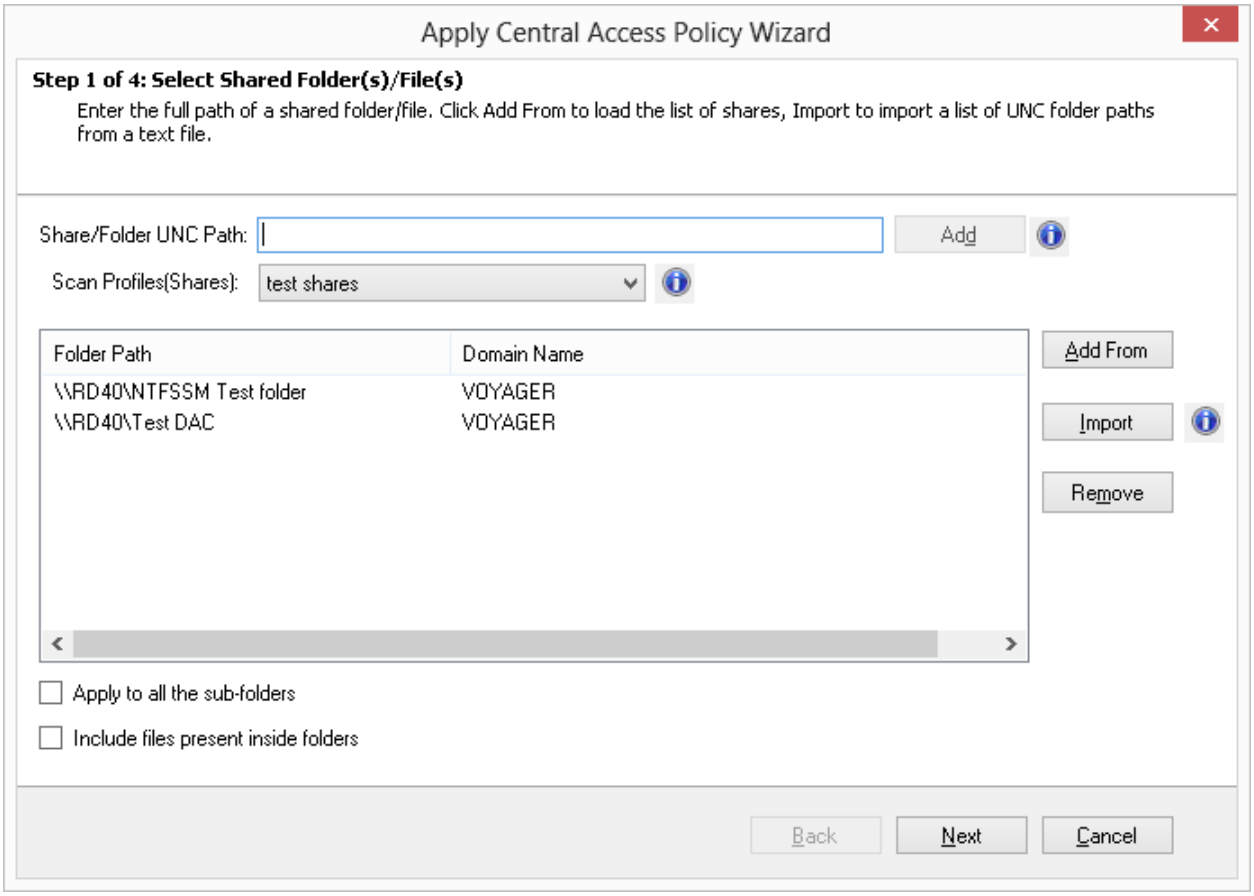
Select shared folder(s)/file(s) by using any of the input options displayed


Apply Central Access Policy Wizard
Step 1 of 4: Select Shared Folder(s)/File(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profiles(Shares):
<No Profile found.>
Folder Path
Domain Name
Add From
Import
Remove
Apply to all the sub-folders
Include files present inside folders
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click Add From option
- Select one or more servers to enumerate its shared folder(s)/file(s)



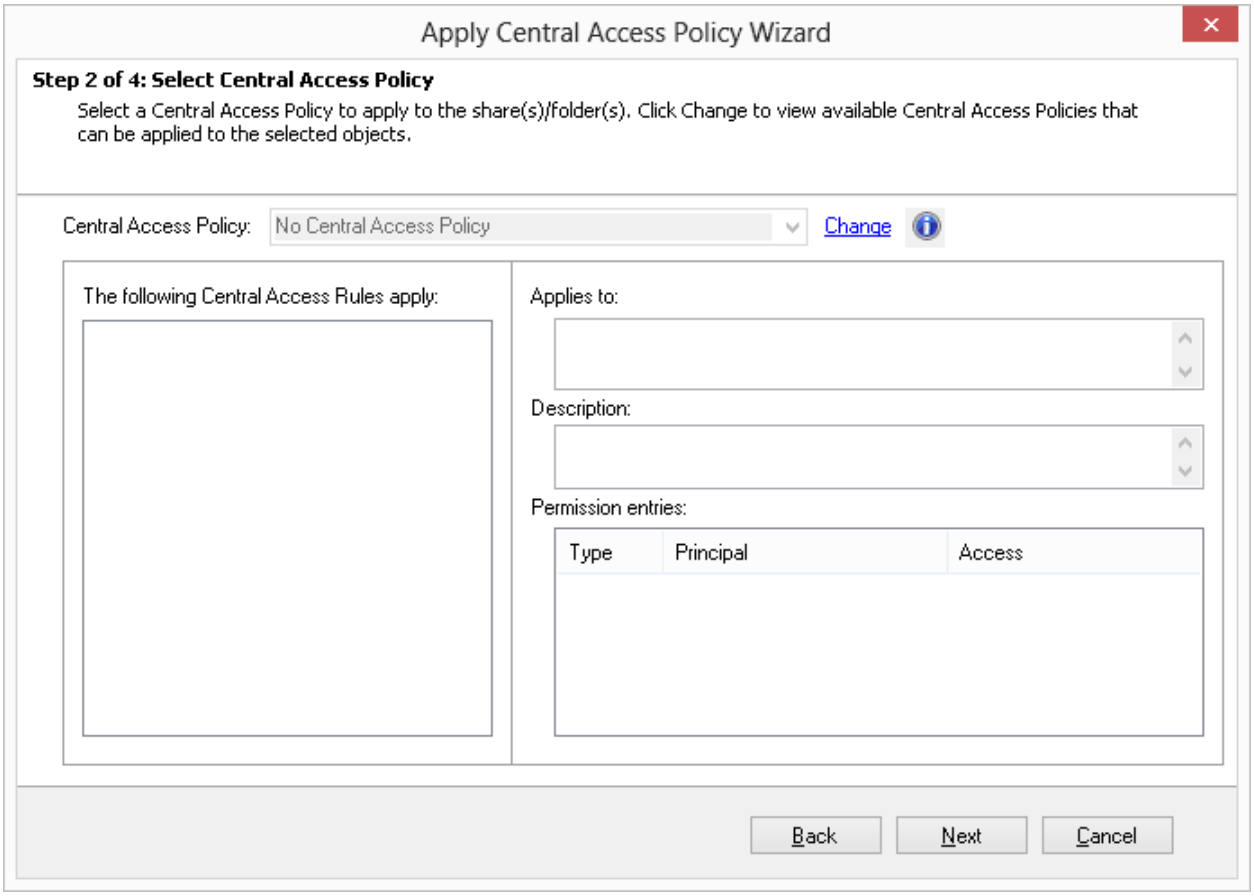
- Use **Select a Scan Profile (Shares)** option to use the shares added in the profile.



- **Apply to all the sub-folders**: This option will apply central access policy on all sub-folders of the selected folders as specified in this wizard.
- **Include files present inside folders**: This option will apply central access policy on all files present in the selected folders as specified in this wizard.

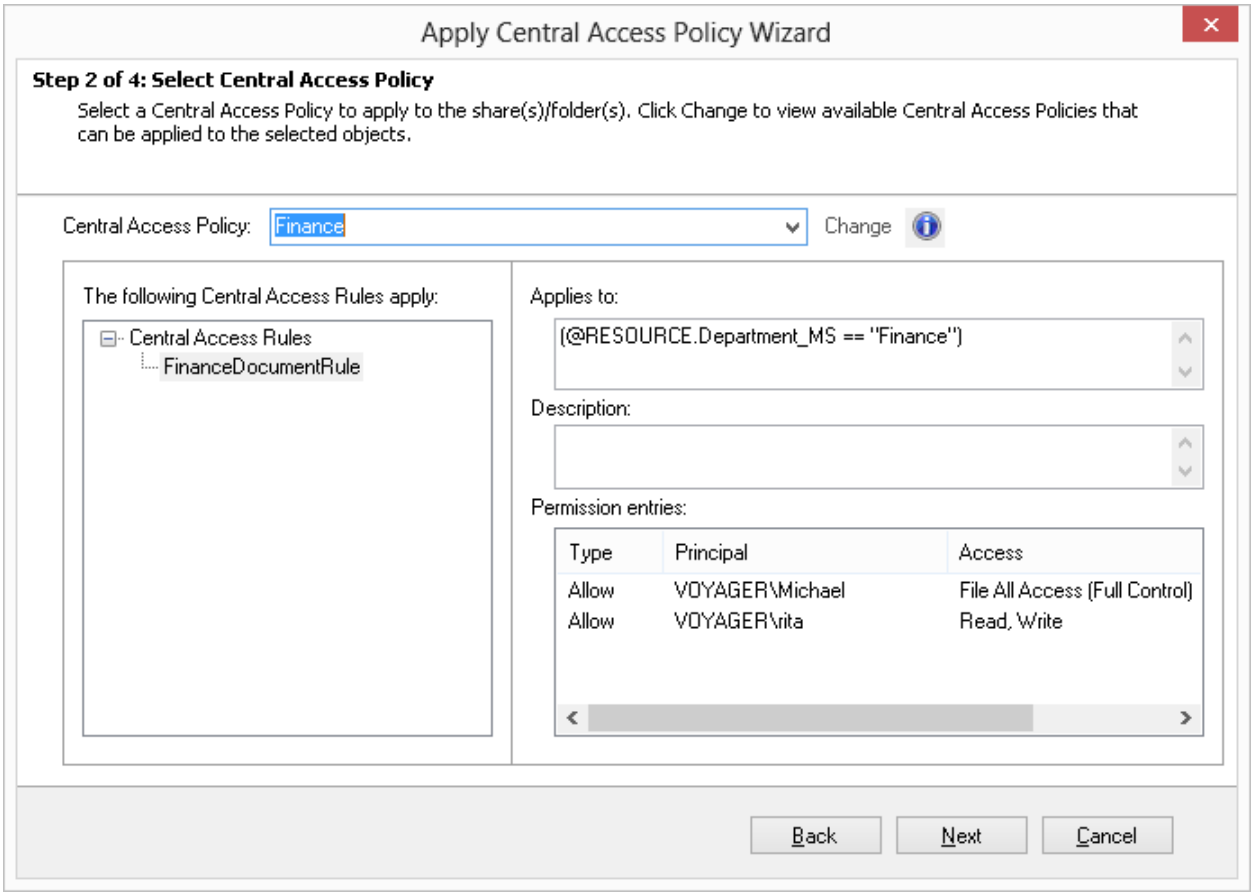
Click **Next** to proceed to the next step.

Step 2: Select Central Access Policy


Apply Central Access Policy Wizard
Step 2 of 4: Select Central Access Policy
Select a Central Access Policy to apply to the share(s)/folder(s). Click Change to view available Central Access Policies that can be applied to the selected objects.
Central Access Policy:
No Central Access Policy
Change
The following Central Access Rules apply:
Applies to:
Description:
Permission entries:
Type
Principal
Access
Back
Next
Cancel

- Click **Change** to view available Central Access Policies that can be applied to the selected shared folders/files.

Note: You must be a member of the selected shares' domain and connected to the shares from a domain-authenticated session to view Central Access Policy information.

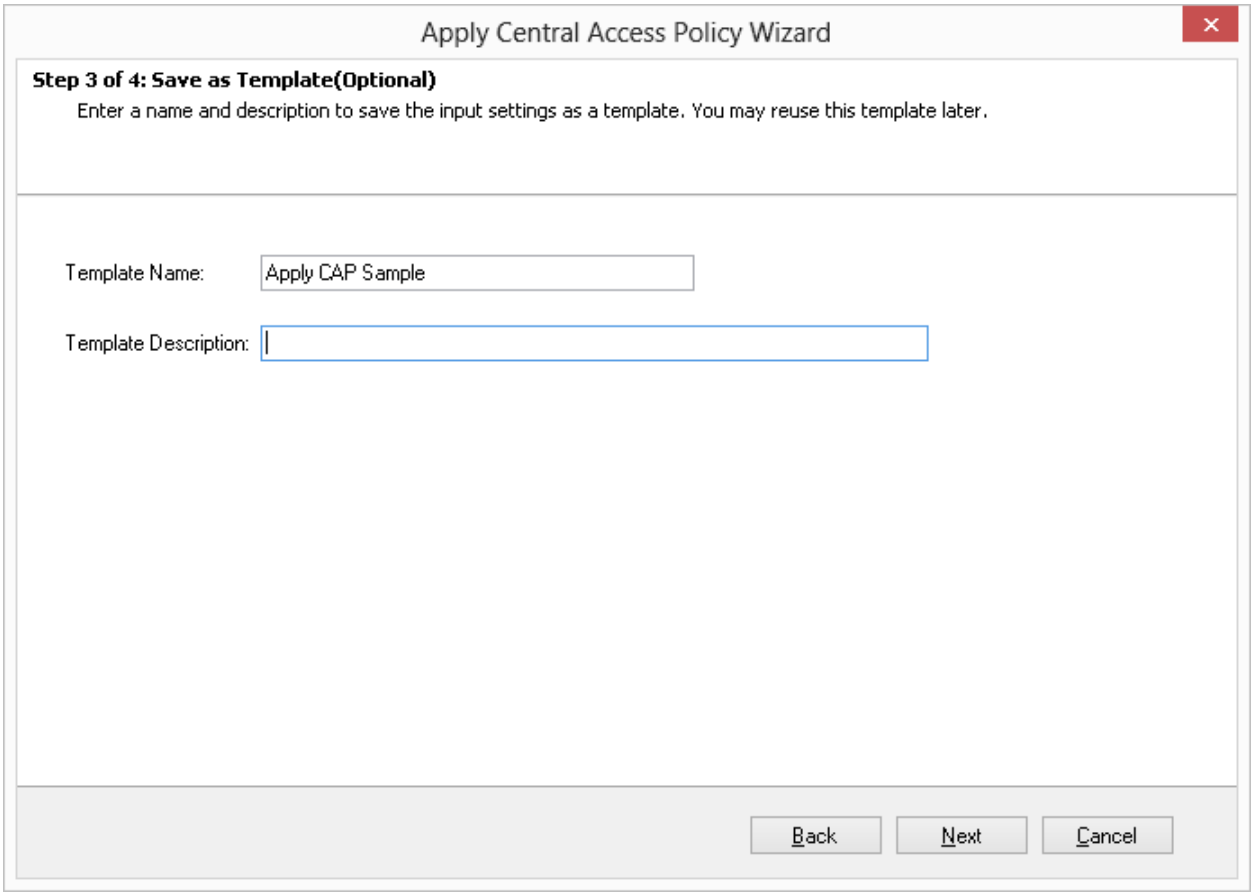


- Select the Central Access Policy from the list of Central Access Policies. After you select the Central Access Policy, a list of Central Access Rules that are members of the selected Central Access Policy will appear in the tree view. You can view the details of the Central Access Rules by selecting the Central Access Rule from the tree view.
- Click **Next** to proceed to the next step.

Step 3: Save as template (Optional)

Enter a name and description to save the input settings as a template. You may reuse this template later.

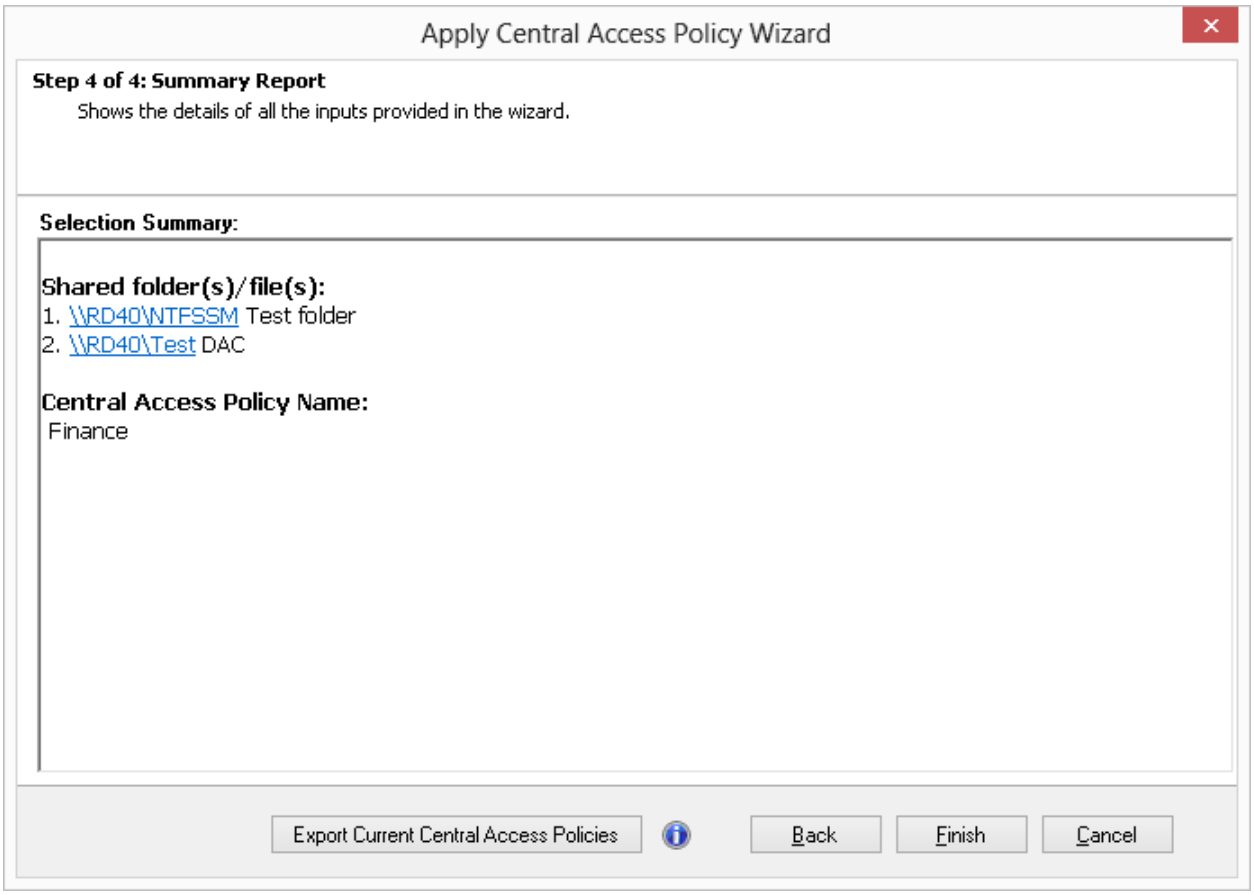
How to reuse the Apply CAP template?


Apply Central Access Policy Wizard
Step 3 of 4: Save as Template(Optional)
Enter a name and description to save the input settings as a template. You may reuse this template later.
Template Name:
Apply CAP Sample
Template Description:
Back
Next
Cancel

Click **Next** to proceed to the next step

Step 6: Summary

This step displays the summary of all the input data along with the selected options.



Click **Finish** to complete the Apply Central Access Policy wizard.

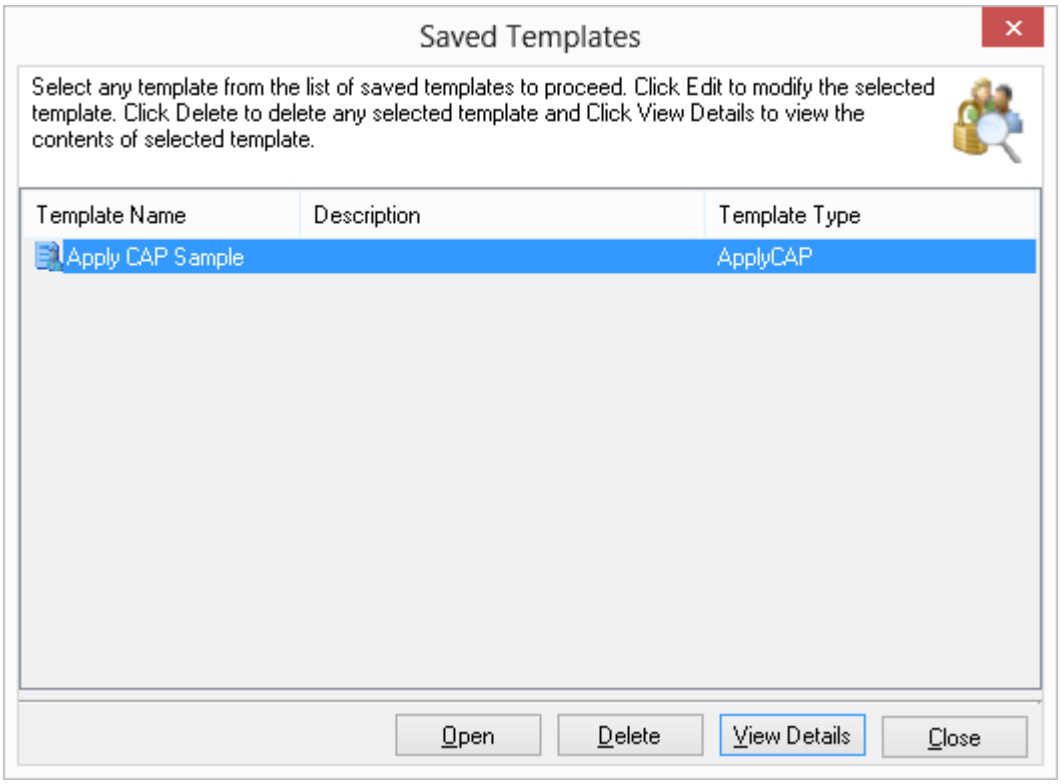
Central Access Policy will be applied as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.

How to reuse the Apply CAP template?

The **Saved Templates** contains the list of saved templates to Apply CAP, Revoke CAP, Grant Permissions, Revoke Permissions and copy Permissions.

Click on

button in the toolbar. The Saved Templates window will be displayed as shown below.


Saved Templates
Select any template from the list of saved templates to proceed. Click Edit to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
Apply CAP Sample
ApplyCAP
Open
Delete
View Details
Close

The saved templates window allows you to perform the following operations:

- Open an existing template
- Delete a template
- Preview the contents of a template

Open an existing Template

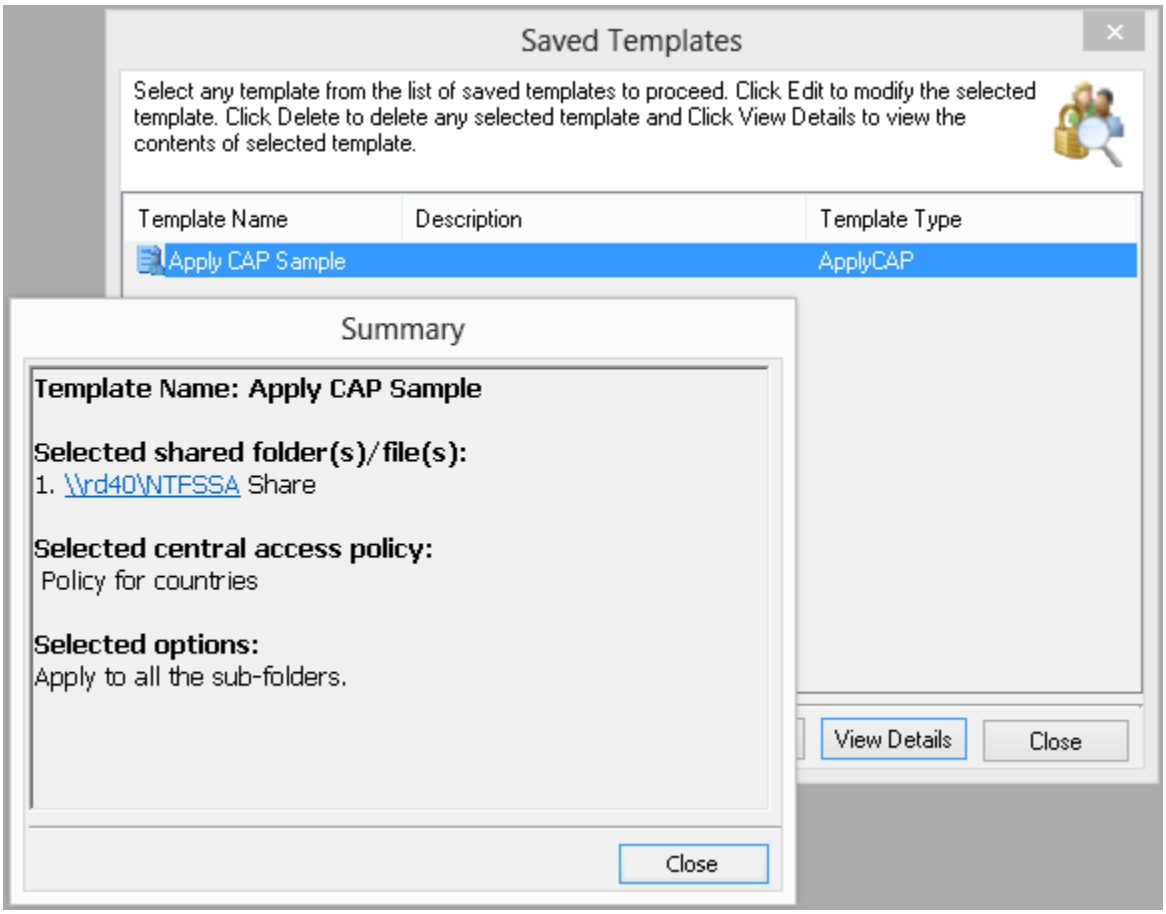
1. To open an existing Apply CAP template, select the Apply CAP template and click **Open** button in the window. The Apply CAP Dialog will appear on the screen which will allow you to edit the selected template.
2. During edit operation you can modify the computer list and central access policy entries, however, you cannot modify the name of the template.

Delete a template

To delete a Apply CAP template, select a Apply CAP template which you want to delete, and then click **Delete** button. The selected template will be deleted permanently.

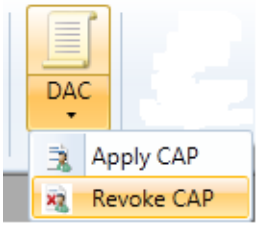
Preview the settings of a Template

To preview the settings of a saved Template, select a saved Apply CAP template, and then click **View Details** button. The settings will be displayed in a window as shown below:


Saved Templates
Select any template from the list of saved templates to proceed. Click Edit to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
Apply CAP Sample
ApplyCAP
Summary
Template Name: Apply CAP Sample
Selected shared folder(s)/file(s):
1. \\rd40\NTFSSA Share
Selected central access policy:
Policy for countries
Selected options:
Apply to all the sub-folders.
Close
View Details
Close

How to Revoke Central Access Policy from the selected Shares?

The **Revoke CAP** feature allows you to remove a central access policy from the shared folders and files. You will also have the option to revoke a central access policy only if the selected central access policy applied on the selected shared folders and files.

Click on 

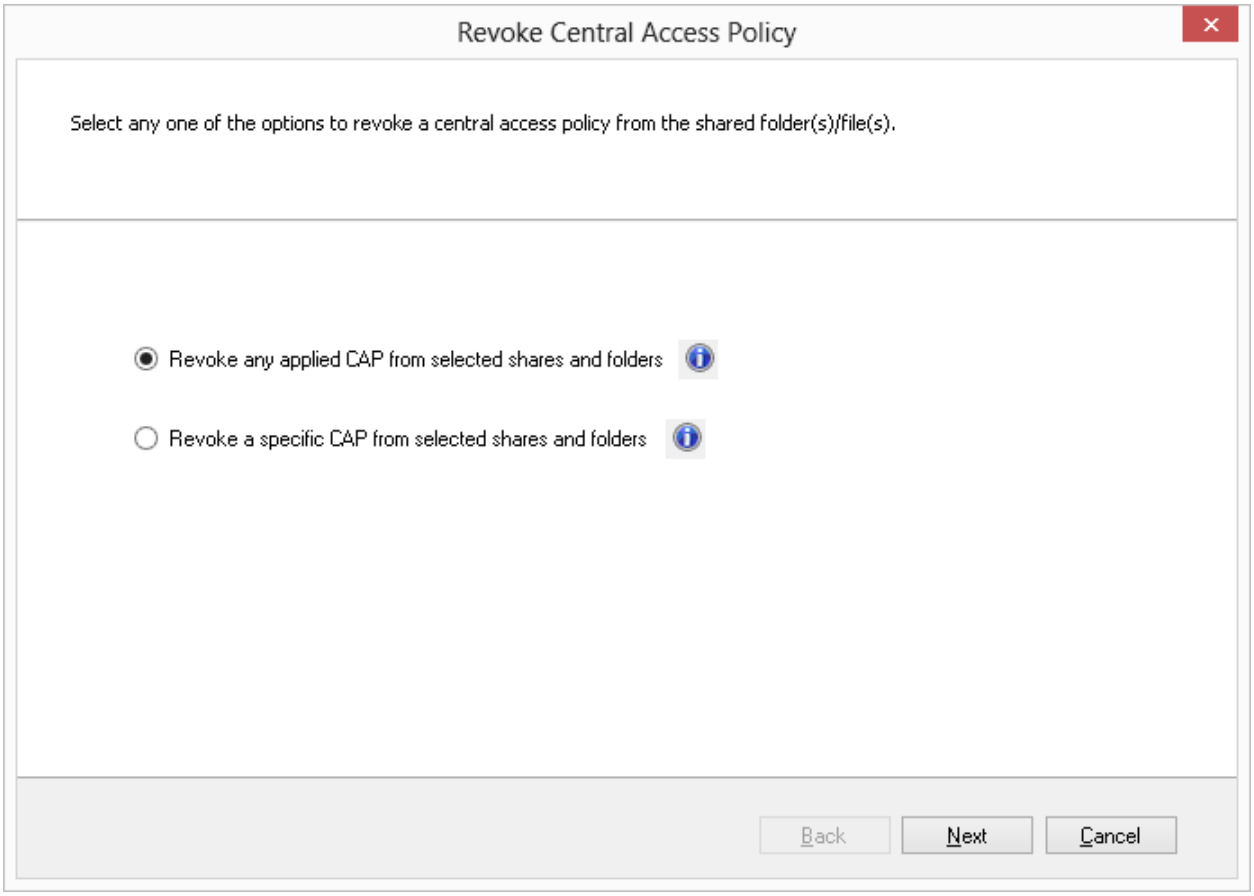
button in the toolbar.

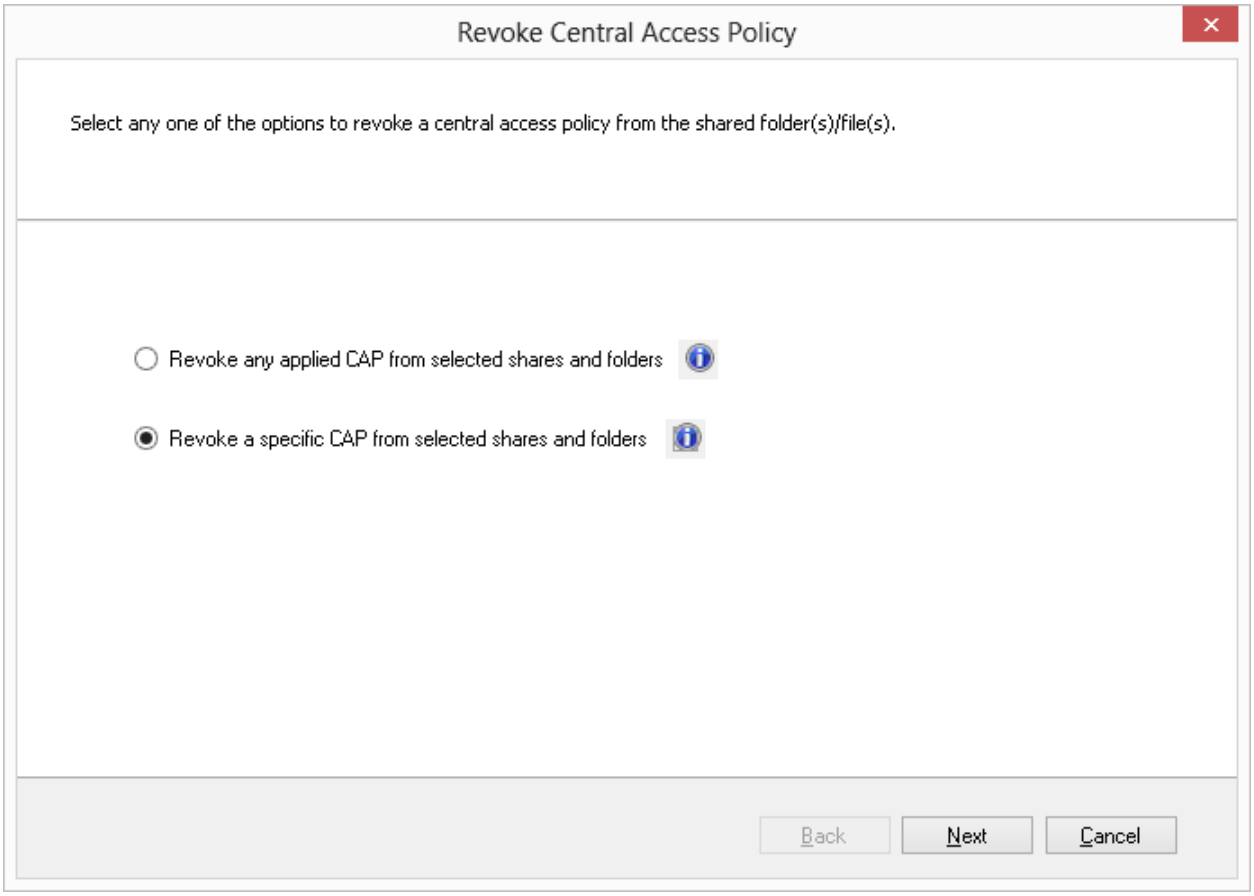
The Revoke CAP window will be displayed as shown below:

Step 1: Select a Revoke CAP option

Select any one of the options below:

- **Revoke any applied CAP from selected shares and folders**: This option will remove a central access policy from the selected shared folder(s)/file(s).
- **Revoke a specific CAP from selected shares and folders**: This option will revoke a central access policy only if the selected central access policy applied on the selected shared folders and files.

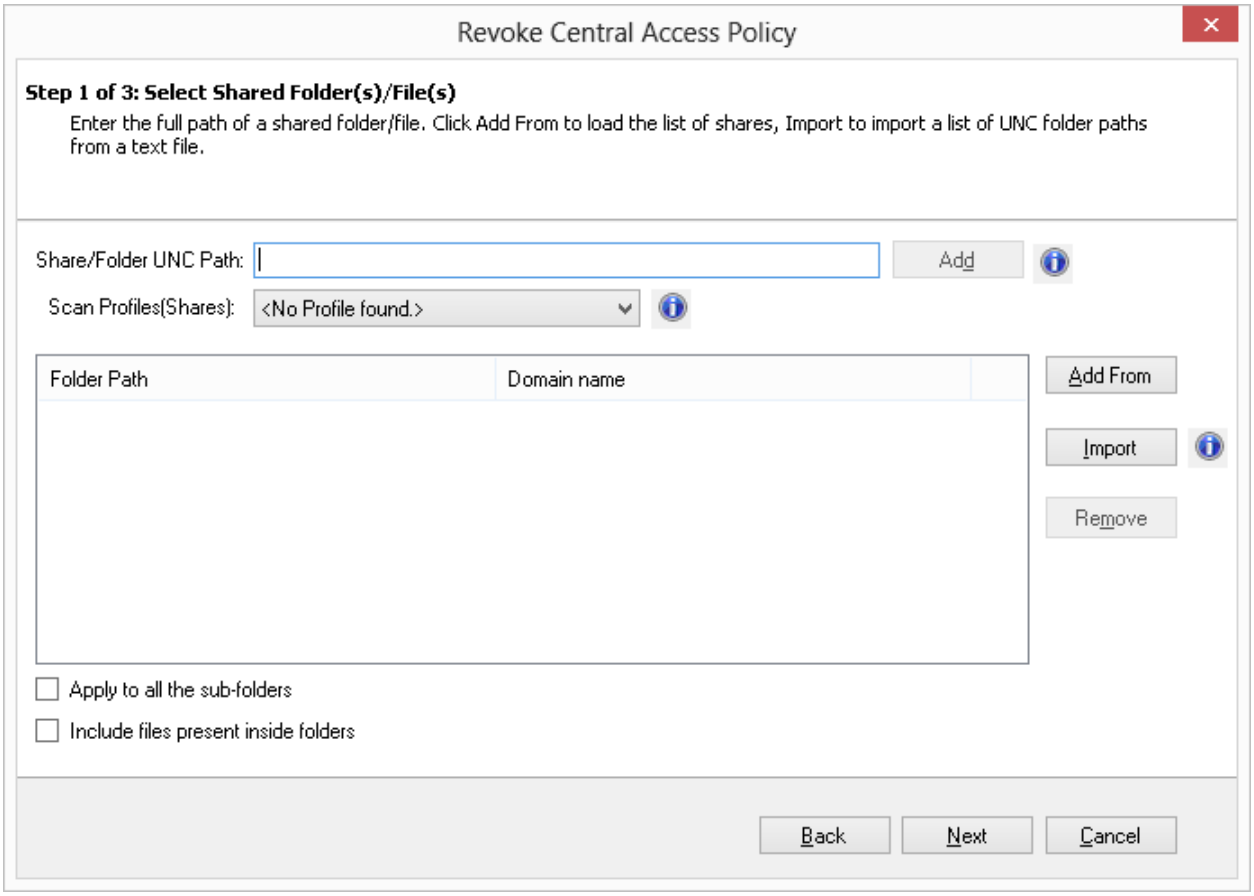

Revoke Central Access Policy
Select any one of the options to revoke a central access policy from the shared folder(s)/file(s).
Revoke any applied CAP from selected shares and folders
Revoke a specific CAP from selected shares and folders
Back
Next
Cancel


Revoke Central Access Policy
Select any one of the options to revoke a central access policy from the shared folder(s)/file(s).
Revoke any applied CAP from selected shares and folders
Revoke a specific CAP from selected shares and folders
Back
Next
Cancel

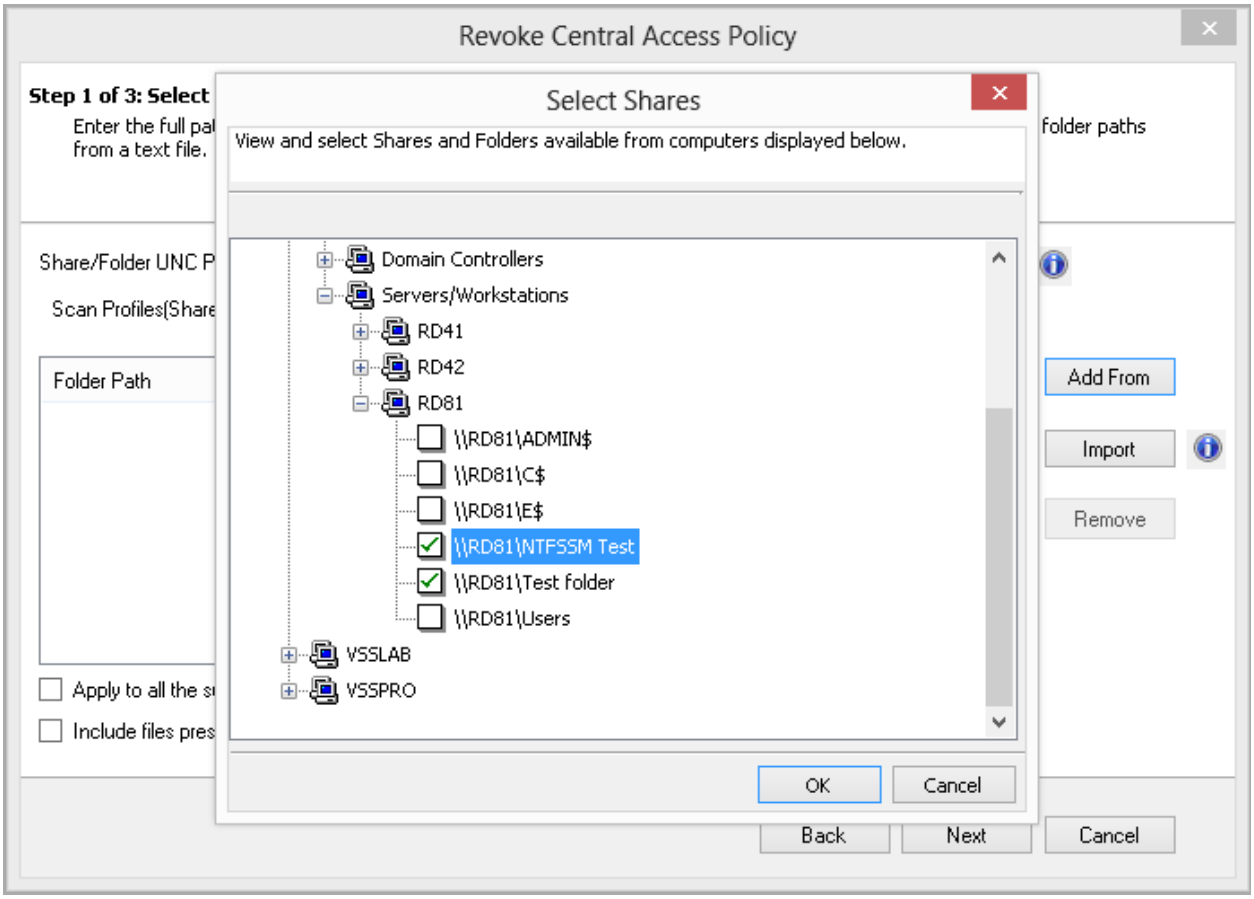
Click **Next** to proceed to the Next step.

Step 2: Select shared folder(s)/file(s)

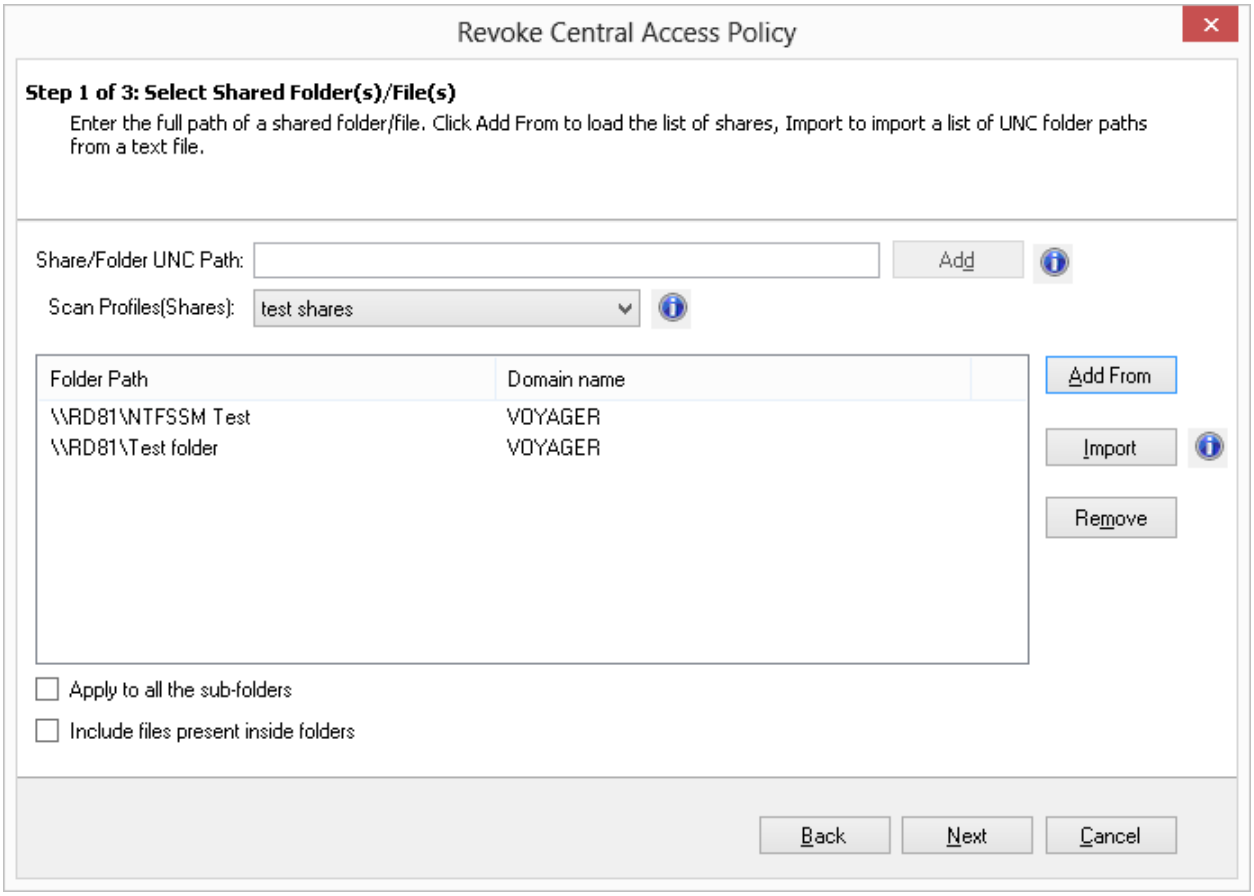
Select shared folder(s)/file(s) by using any of the input options displayed.


Revoke Central Access Policy
Step 1 of 3: Select Shared Folder(s)/File(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profiles(Shares):
<No Profile found.>
Folder Path
Domain name
Add From
Import
Remove
Apply to all the sub-folders
Include files present inside folders
Back
Next
Cancel

- If you want to select shares from servers for which you wish to add, then click **Add From** option
- Select one or more servers to enumerate its shared folder(s)/file(s)



- Use **Select a Scan Profile (Shares)** option to use the Shares added in the profile.

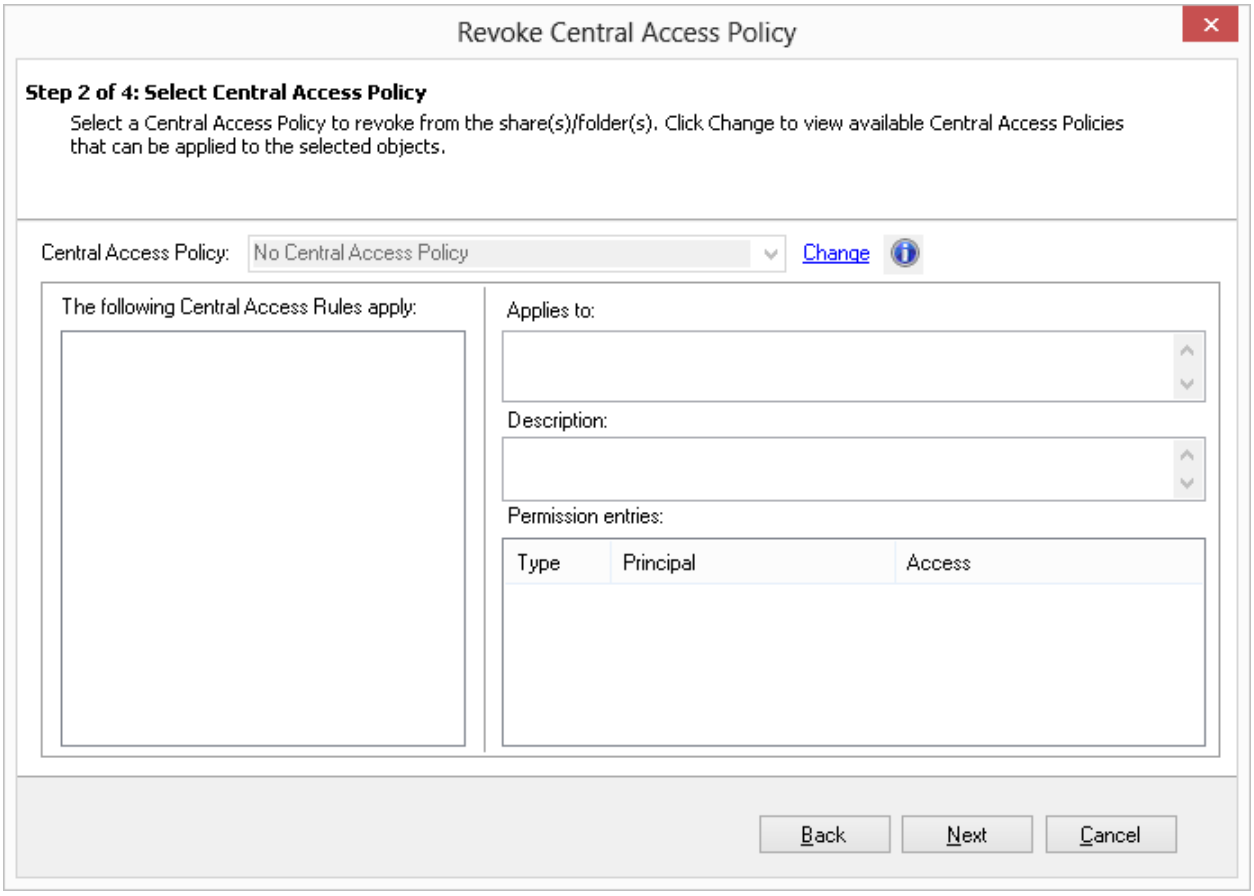


You may also type the UNC path of a folder that is not in the list, such as a folder that is shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

- **Apply to all the sub-folders**: This option will revoke central access policy from all sub-folders of the selected folders as specified in this wizard.
- **Include files present inside folders**: This option will revoke central access policy from all files present in the selected folders as specified in this wizard.

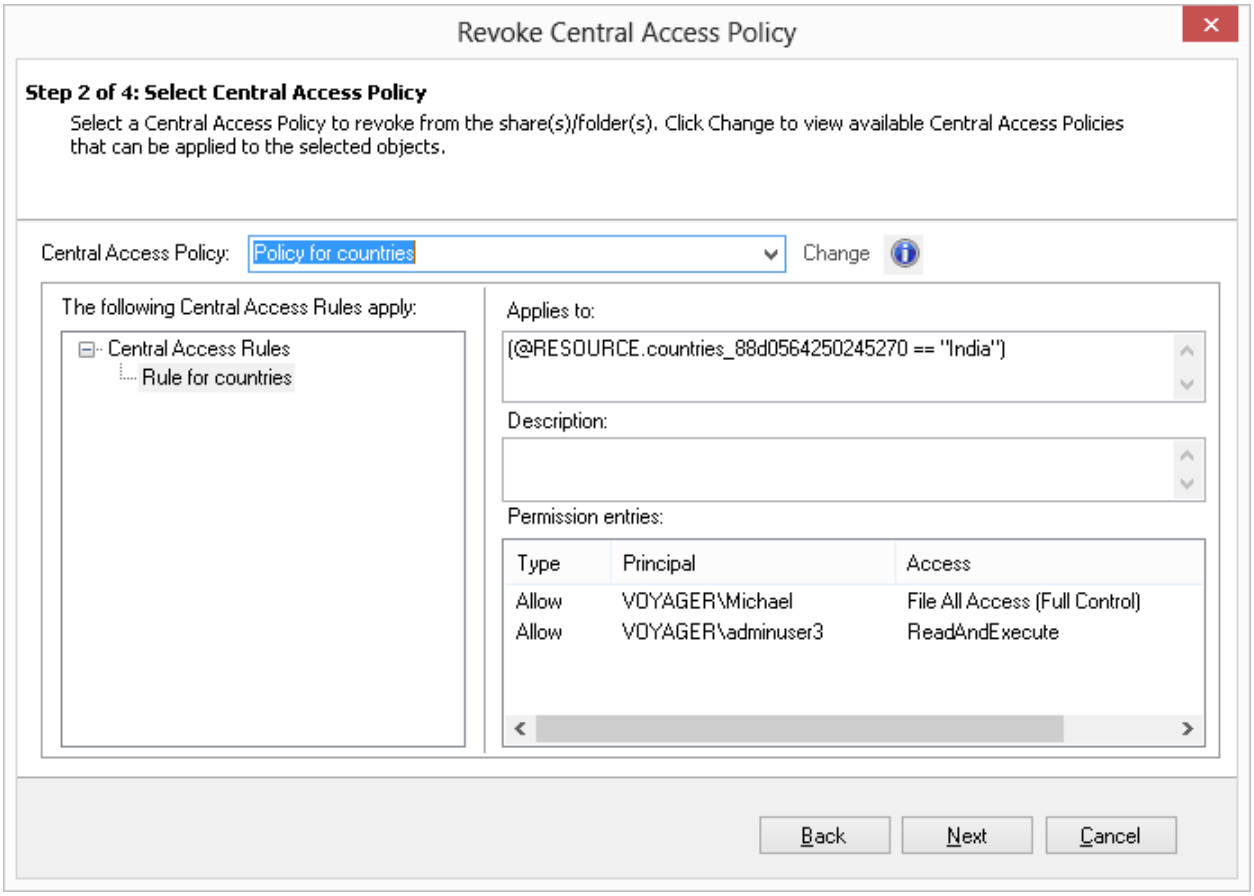
Click **Next** to proceed to the Next step.

Step 3: Select Central Access Policy



- Click **Change** to view available Central Access Policies that can be applied to the selected shared folders/files.

Note: You must be a member of the selected shares' domain and connected to the shares from a domain-authenticated session to view Central Access Policy information.

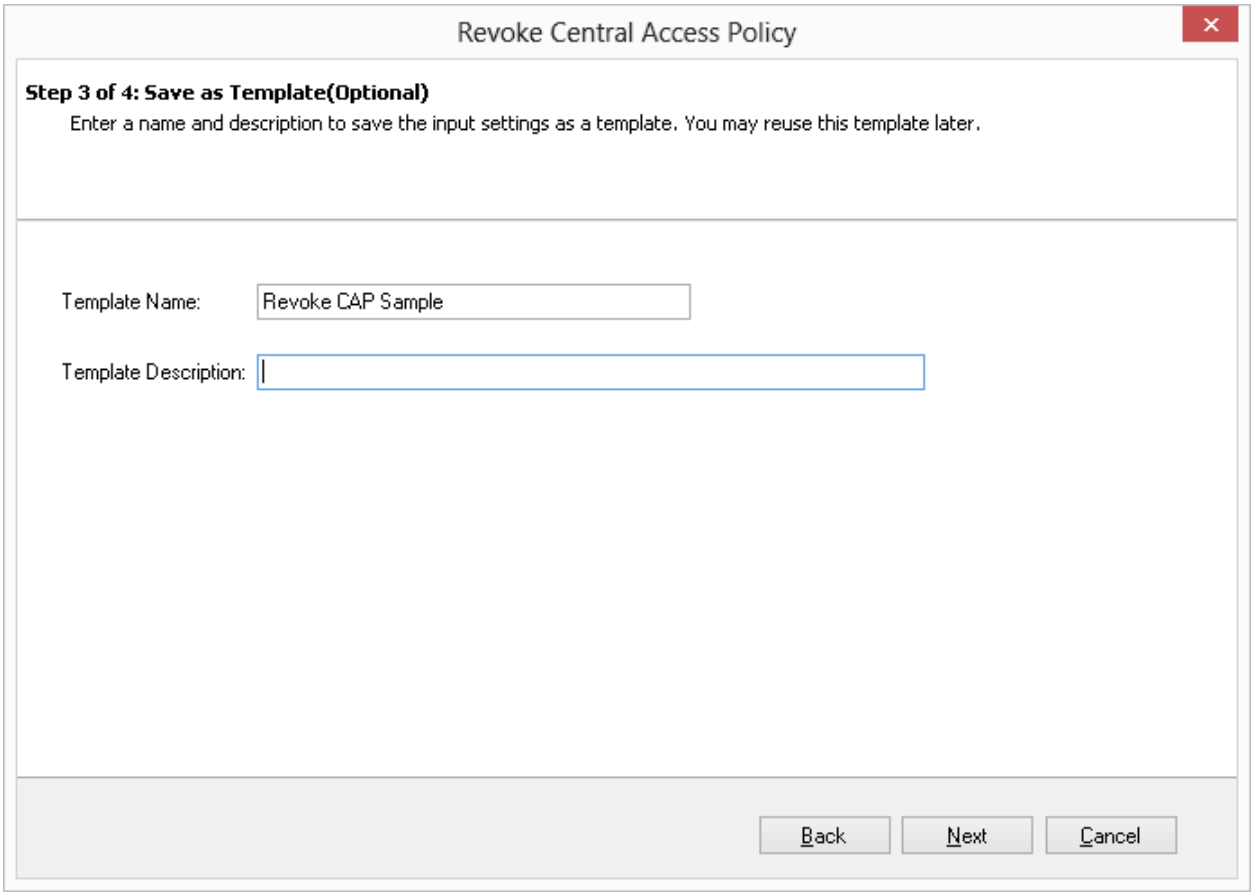


- Select the Central Access Policy from the list of Central Access Policies. After you select the Central Access Policy, a list of Central Access Rules that are members of the selected Central Access Policy will appear in the tree view. You can view the details of the Central Access Rules by selecting the Central Access Rule from the tree view.
- Click **Next** to proceed to the next step.

Step 4: Save as template

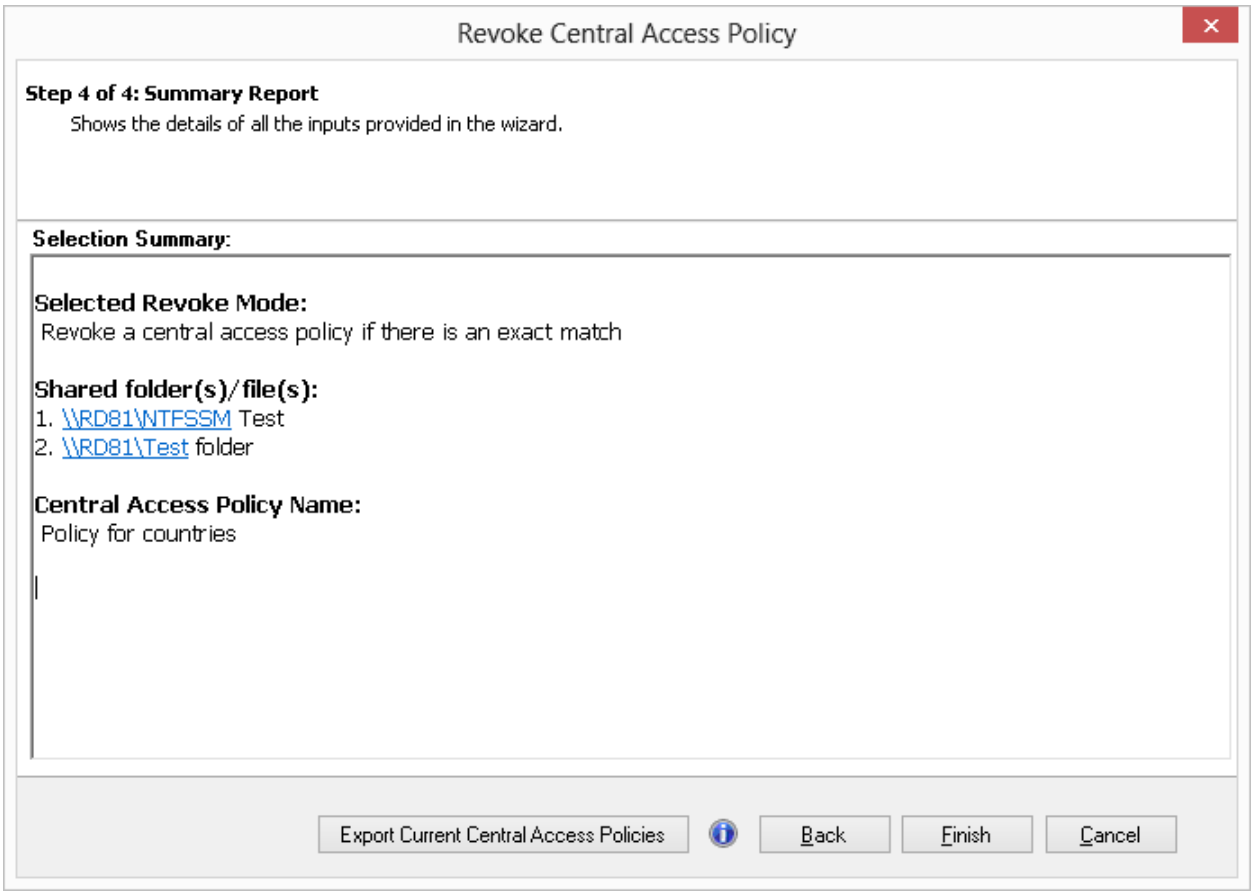
Enter a name and description to save the input settings as a template. You can reuse this template later.

How to reuse the Revoke CAP template?


Revoke Central Access Policy
Step 3 of 4: Save as Template(Optional)
Enter a name and description to save the input settings as a template. You may reuse this template later.
Template Name:
Revoke CAP Sample
Template Description:
Back
Next
Cancel

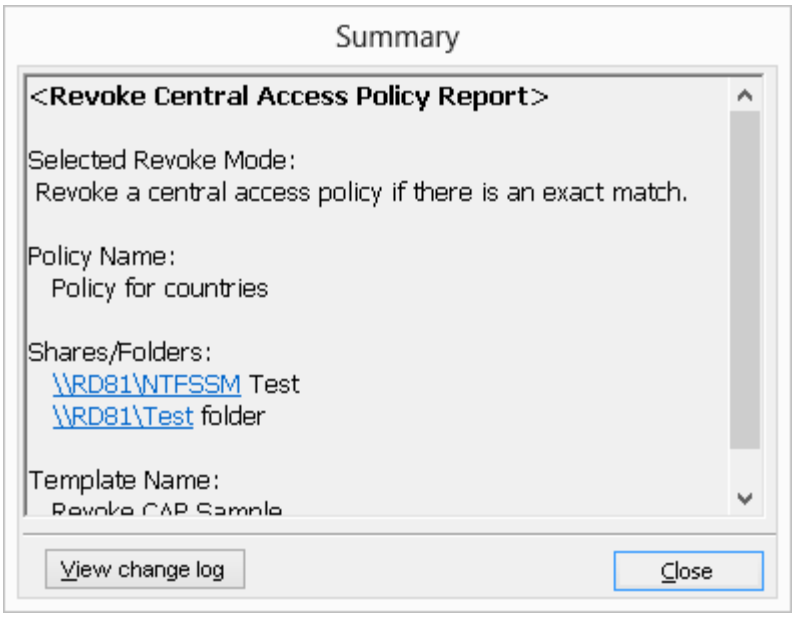
Step 5: Selection Summary

This step displays the summary of data selected to Revoke CAP and you can also view and export the existing central access policy before changes are applied, by clicking on the **Export Current Central Access Policies** button.


Revoke Central Access Policy
Step 4 of 4: Summary Report
Shows the details of all the inputs provided in the wizard.
Selection Summary:
Selected Revoke Mode:
Revoke a central access policy if there is an exact match
Shared folder(s)/file(s):
1. \\RD81\NTFSSM Test
2. \\RD81\Test folder
Central Access Policy Name:
Policy for countries
Export Current Central Access Policies
Back
Finish
Cancel

Click **Finish** to complete the Revoke CAP wizard.

Central Access Policy will be revoked as specified in the wizard. The summary of all the input data would be shown below along with the "View change log" option to view the task completion status.

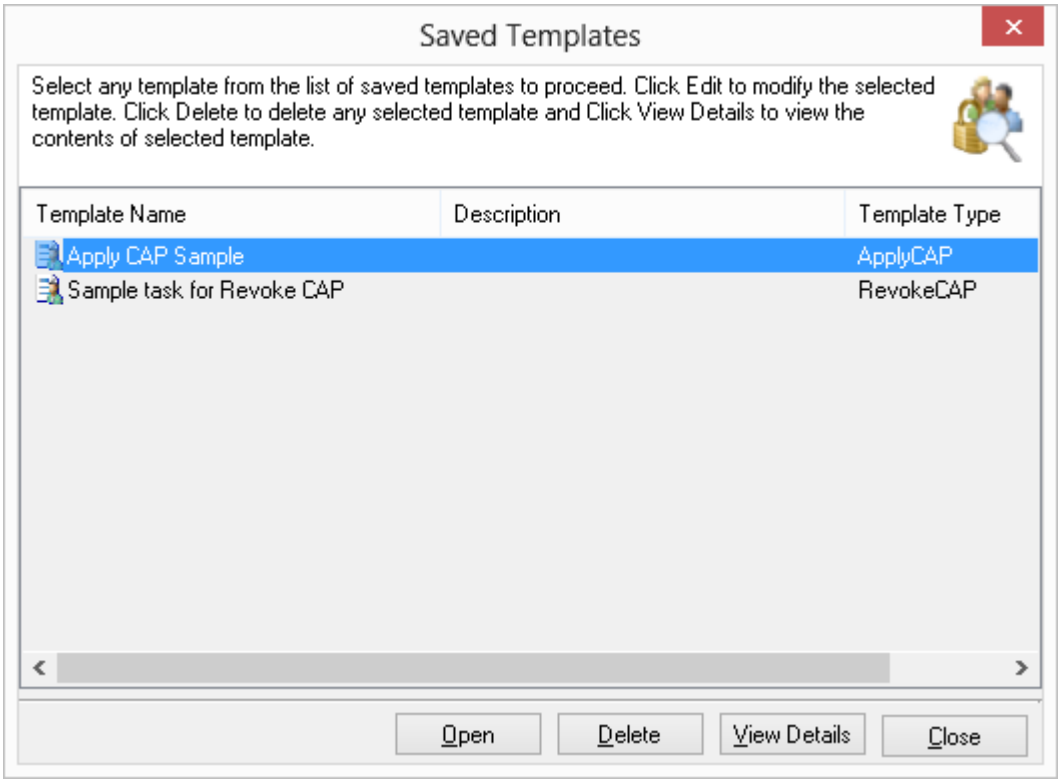

Summary
<Revoke Central Access Policy Report>
Selected Revoke Mode:
Revoke a central access policy if there is an exact match.
Policy Name:
Policy for countries
Shares/Folders:
\\RD81\NTFSSM Test
\\RD81\Test folder
Template Name:
View change log
Close

How to reuse the Revoke CAP template?

The Saved Templates contains the list of saved templates to Apply CAP, Revoke CAP, Grant Permissions, Revoke Permissions and copy Permissions.

Click on

button in the toolbar. The Saved Templates window will be displayed as shown below.


Saved Templates
Select any template from the list of saved templates to proceed. Click Edit to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
Apply CAP Sample
ApplyCAP
Sample task for Revoke CAP
RevokeCAP
Open
Delete
View Details
Close

The saved templates window allows you to perform the following operations:

- Open an existing template
- Delete a template
- Preview the contents of a template

Open an existing Template

1. To open an existing Revoke CAP template, select the Revoke CAP template and click **Open** button in the window. The Revoke CAP Dialog will appear on the screen which will allow you to edit the selected template.

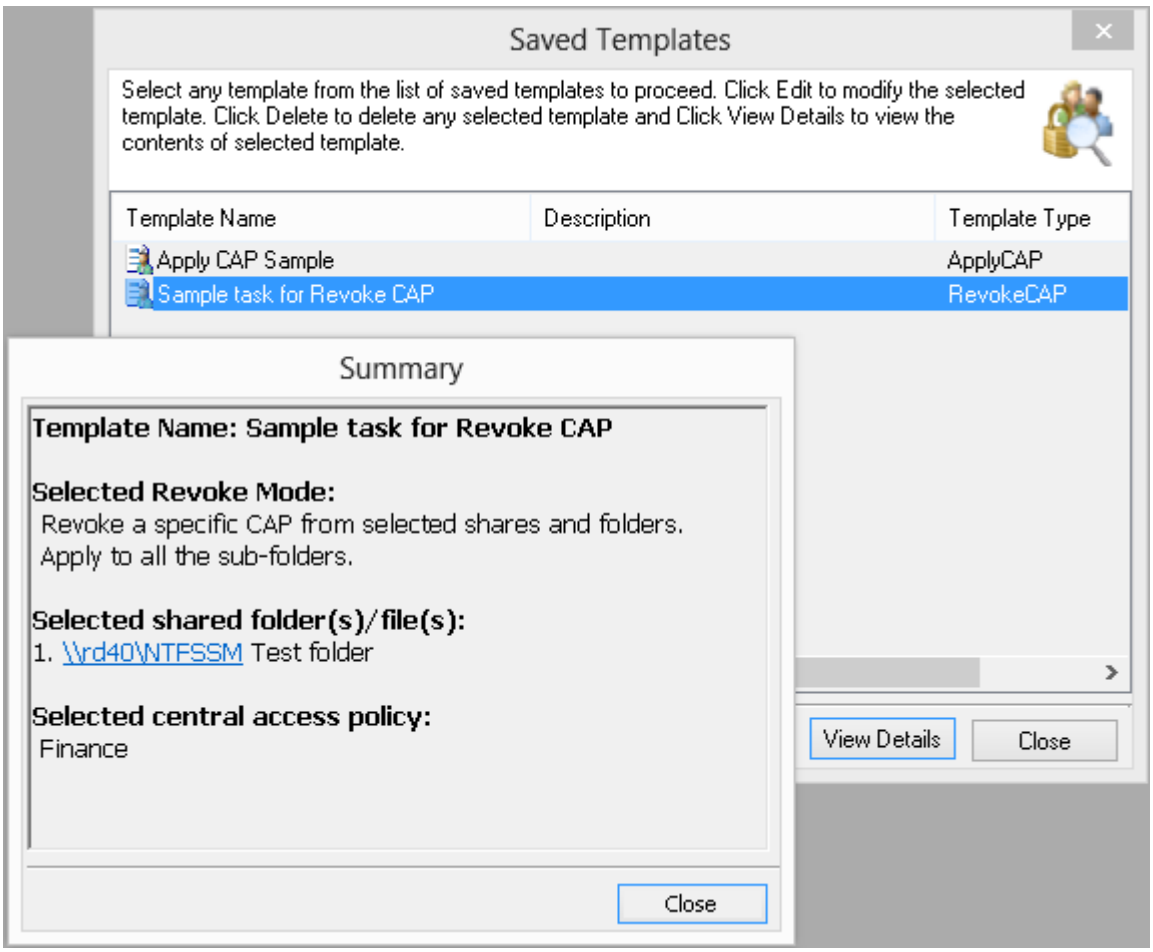
2. During edit operation you can modify the computer list and central access policy entries, however, you cannot modify the name of the template.

Delete a template

To delete a Revoke CAP template, select a Revoke CAP template which you want to delete, and then click **Delete** button. The selected template will be deleted permanently.

Preview the settings of a Template

To preview the settings of a saved Template, select a saved Revoke CAP template, and then click **View Details** button. The settings will be displayed in a window as shown below:


Saved Templates
Select any template from the list of saved templates to proceed. Click Edit to modify the selected template. Click Delete to delete any selected template and Click View Details to view the contents of selected template.
Template Name
Description
Template Type
Apply CAP Sample
ApplyCAP
Sample task for Revoke CAP
RevokeCAP
Summary
Template Name: Sample task for Revoke CAP
Selected Revoke Mode:
Revoke a specific CAP from selected shares and folders.
Apply to all the sub-folders.
Selected shared folder(s)/file(s):
1. \\rd40\NTFSSM Test folder
Selected central access policy:
Finance
Close
View Details
Close

Power Search

About Power Search

How to view Power Search Permissions (DACL) Reports?

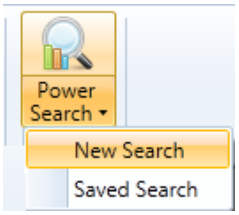
How to manage Power Search?

About Power Search

The Power Search feature lets you perform powerful, conditional Search queries of NTFS Permissions on Files and Folders. You may select specific permissions from the list of standard permissions and Advanced (special) permissions and run a query to determine who have these permissions on which folders and files. You may Save frequently used queries for reuse them later. Here are some examples of how you may make effective use of this feature:

1. Search on who has Full Control on which folders and files
2. Select a set of accounts and determine for which folders and files they have Full control access.
3. Determine which accounts have modify or delete permissions on critical files and folders.
4. Determine what type of permissions members of the Administrators group have on specific folders and files.
5. Determine where Inheritance from Parent folder has been explicitly removed.
6. Determine Accounts for which folders have explicit Allows or Denys set on them.

How to view Power Search Permissions (DACL) Reports?

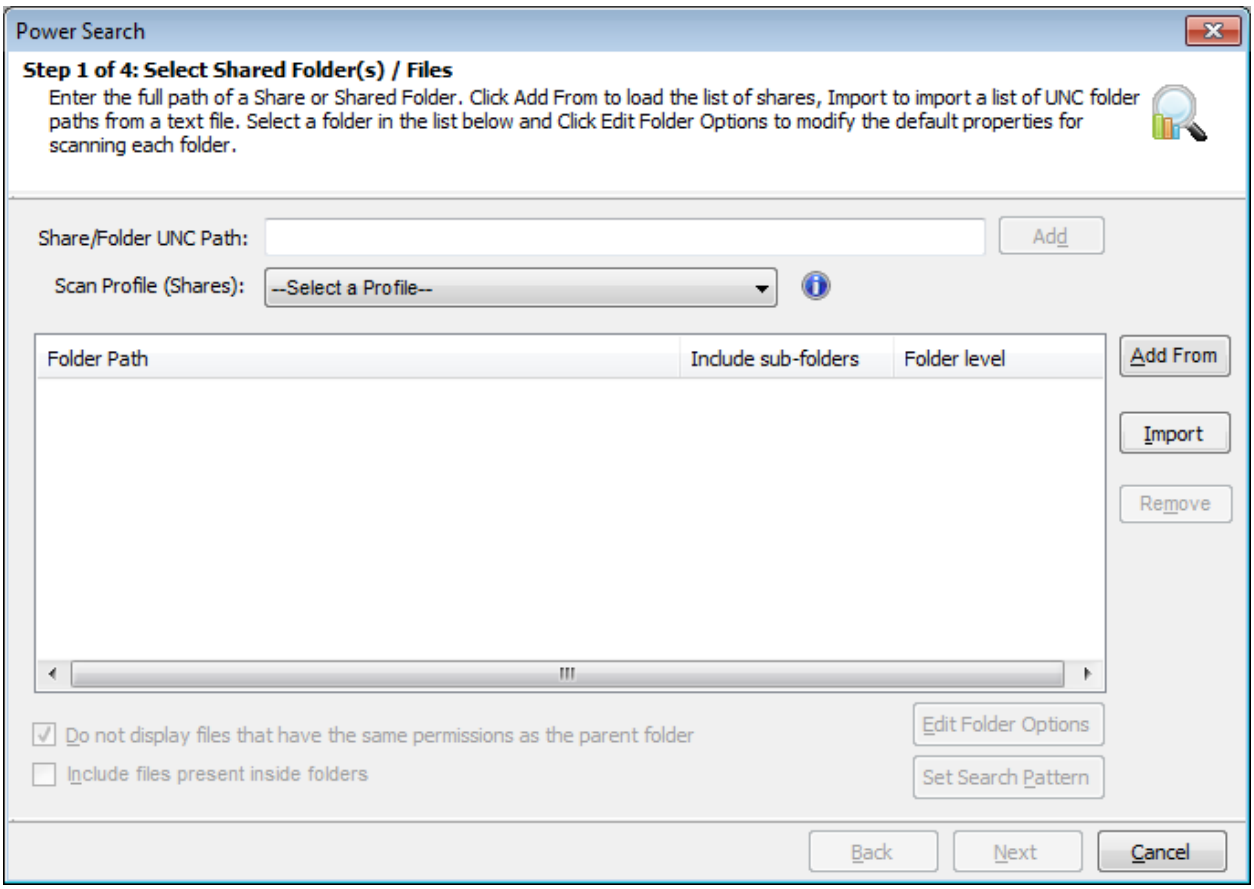
Click on 

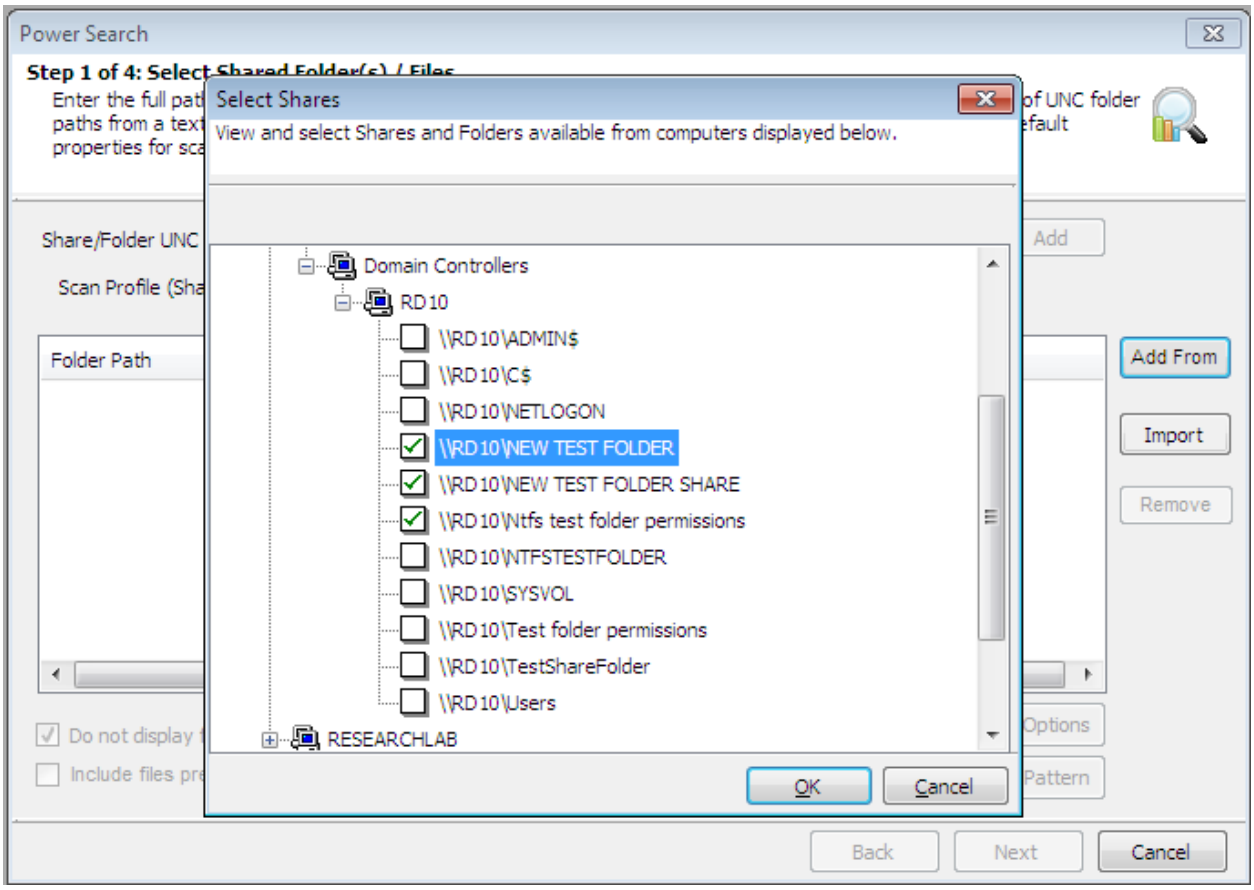
button under Power Search->New Search in button in the toolbar.

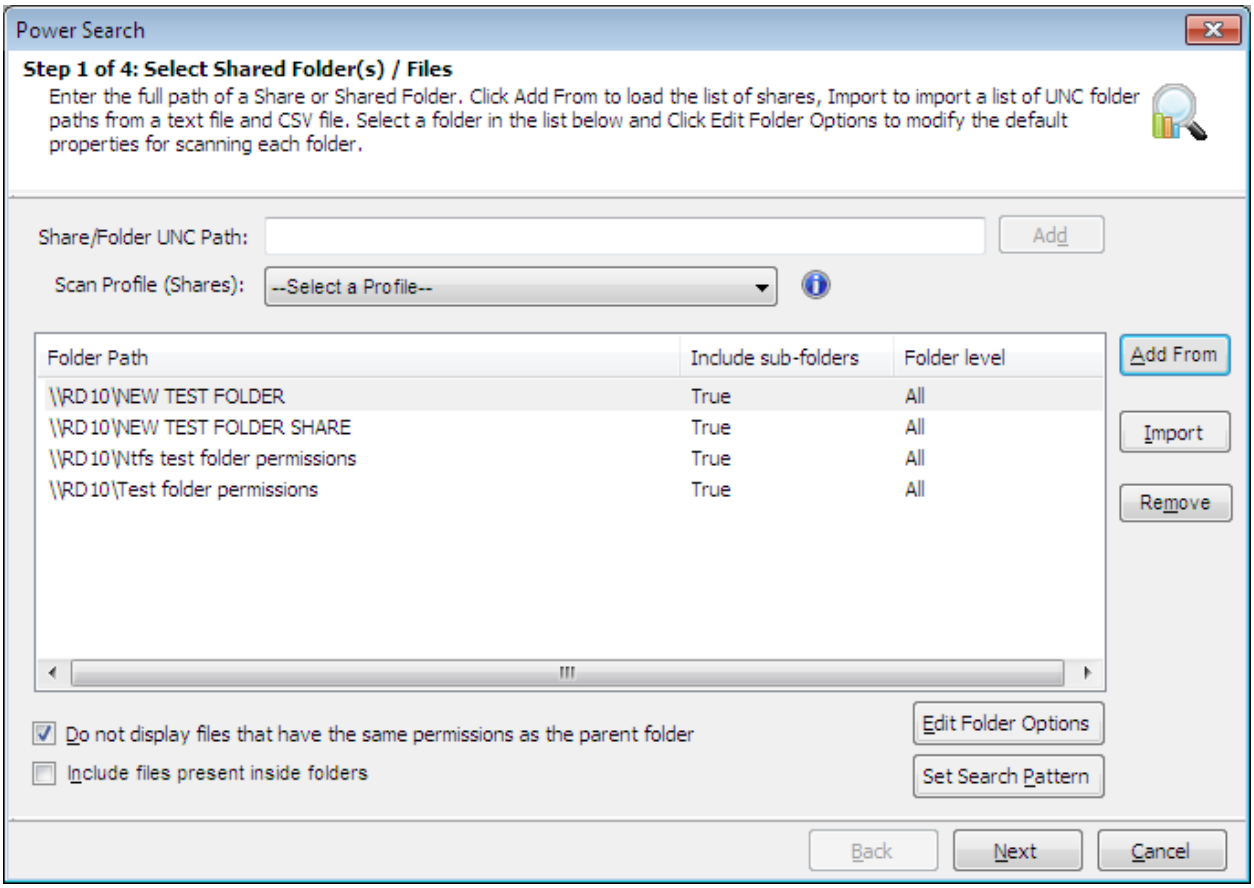
The Power Search window will be displayed as shown below:

Step 1: Select Shared Folder(s)/File(s)

Select one or more servers to enumerate its Shared Folder(s)/File(s)


Power Search
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Edit Folder Options
Set Search Pattern
Back
Next
Cancel


Power Search
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full pat
paths from a text
properties for sca
of UNC folder
efault
Share/Folder UNC
Add
Scan Profile (Sha
Folder Path
Add From
Import
Remove
Do not display
Include files pre
Options
Pattern
Back
Next
Cancel
Select Shares
View and select Shares and Folders available from computers displayed below.
Domain Controllers
RD10
\\RD10\ADMIN$
\\RD10\C$
\\RD10\NETLOGON
\\RD10\NEW TEST FOLDER
\\RD10\NEW TEST FOLDER SHARE
\\RD10\Ntfs test folder permissions
\\RD10\NTFSTESTFOLDER
\\RD10\SYSVOL
\\RD10\Test folder permissions
\\RD10\TestShareFolder
\\RD10\Users
RESEARCHLAB
OK
Cancel

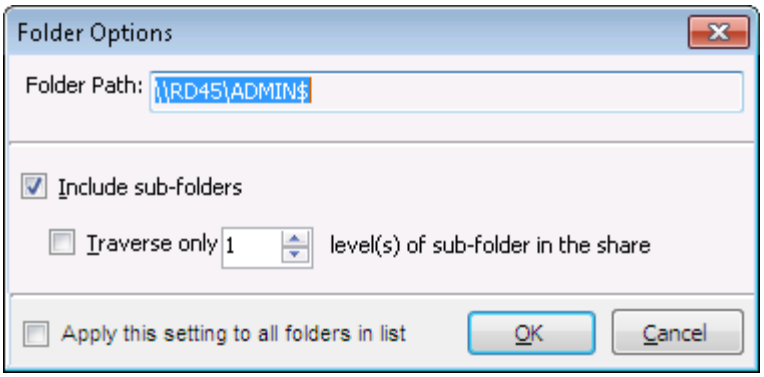

Power Search
Step 1 of 4: Select Shared Folder(s) / Files
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file and CSV file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
\\RD10\NEW TEST FOLDER
True
All
\\RD10\NEW TEST FOLDER SHARE
True
All
\\RD10\Ntfs test folder permissions
True
All
\\RD10\Test folder permissions
True
All
Add From
Import
Remove
Do not display files that have the same permissions as the parent folder
Include files present inside folders
Edit Folder Options
Set Search Pattern
Back
Next
Cancel

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

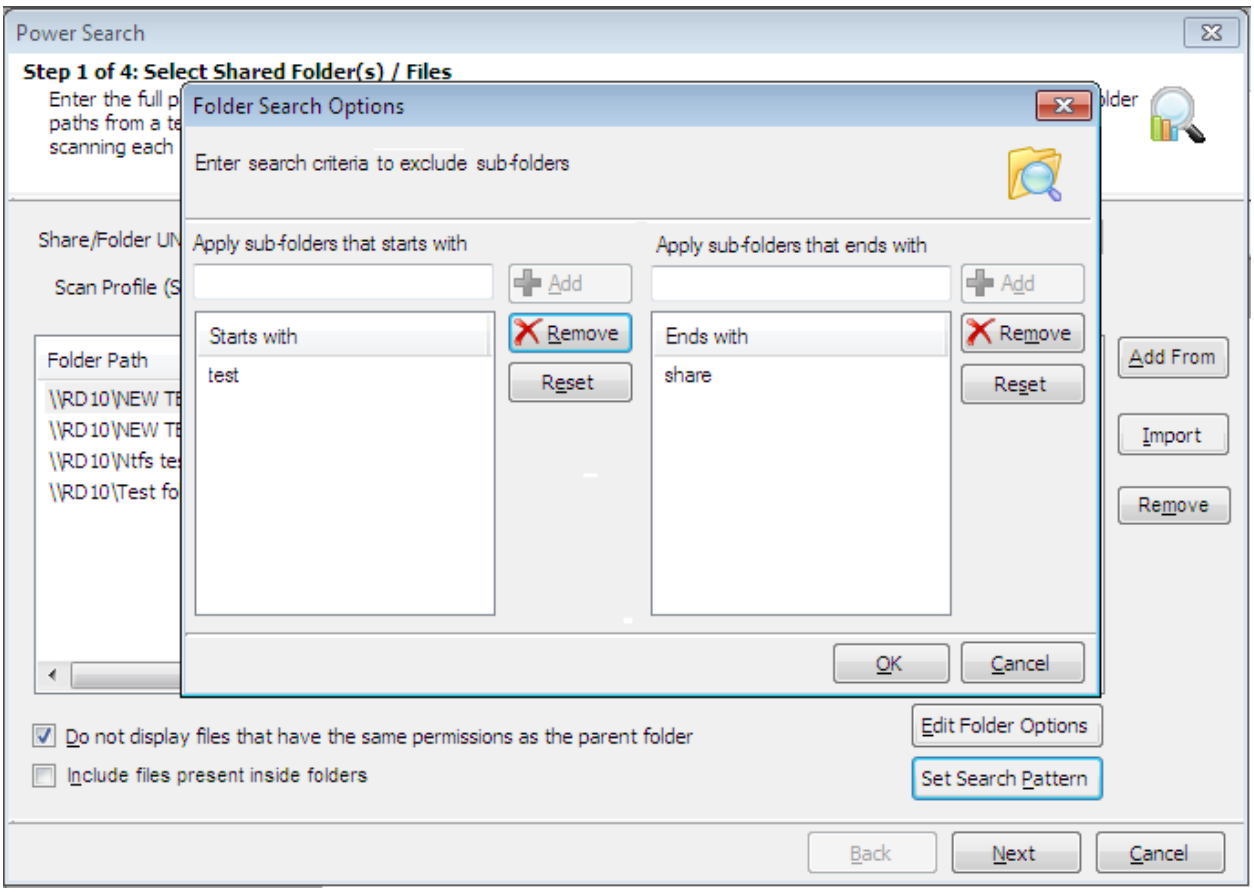
Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select Do not display folders that have same permissions as the parent folder option. This option will not report folders with identical permissions as the parent folder.

Note: The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

NTFS Security Manager defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



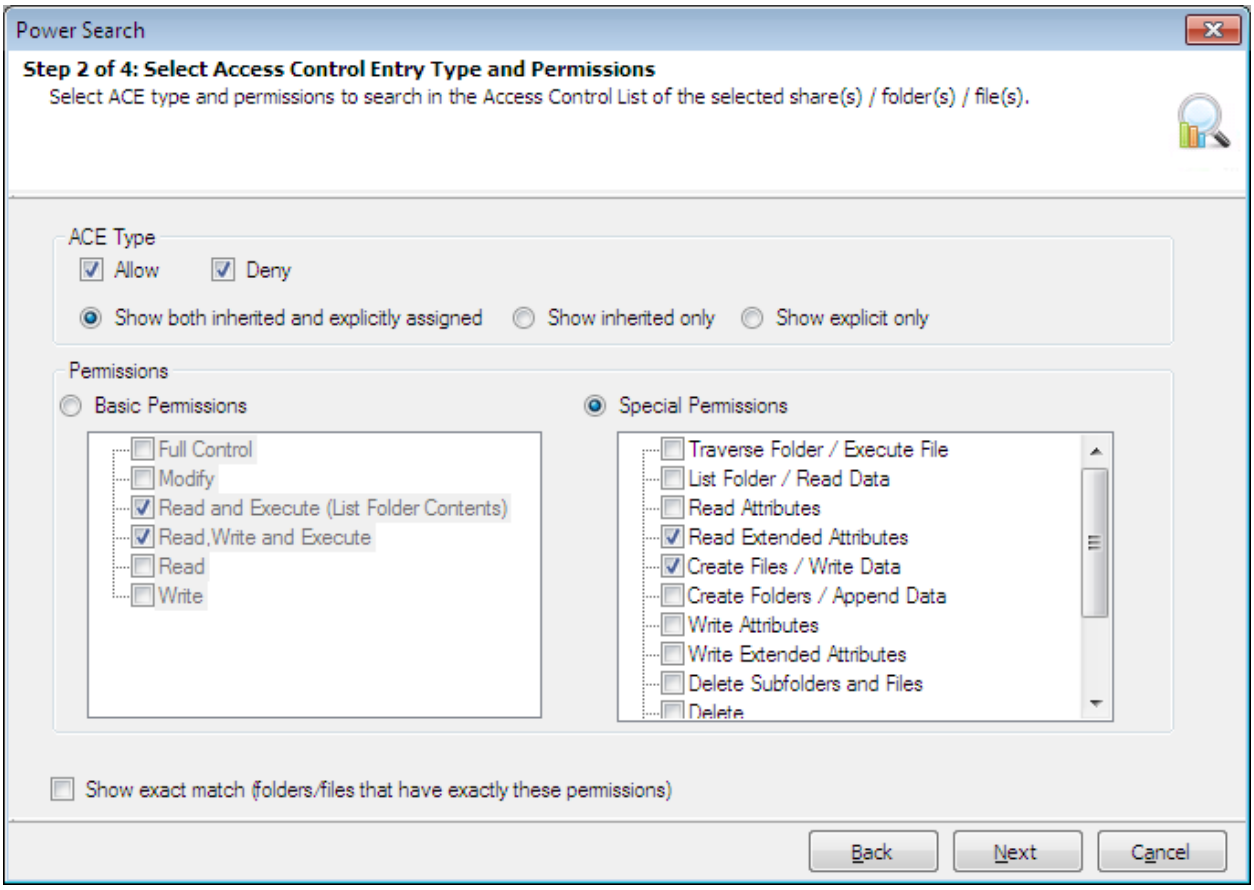
Use **Set Search Pattern** option to exclude sub-folders that match certain pre-defined conditions like Folder name starts with, Folder name ends with. Example: Folder name starts with test, Folder name ends with share.



Click **Next** to proceed to the next step.

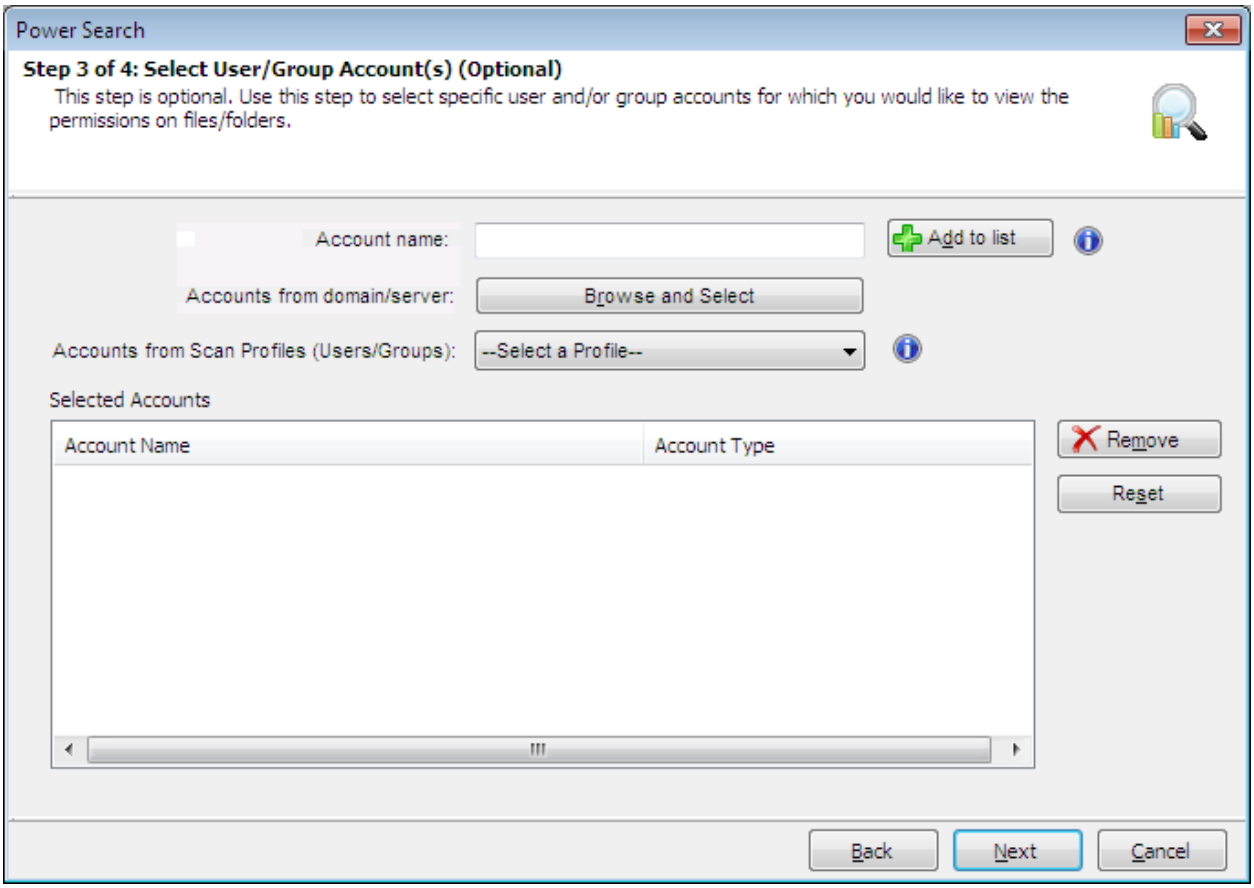
Step 2: Select Access Control Entry Type and Permissions

Select ACE Type and permissions to search in the Access Control List of the selected share(s) / folder(s) /files(s)

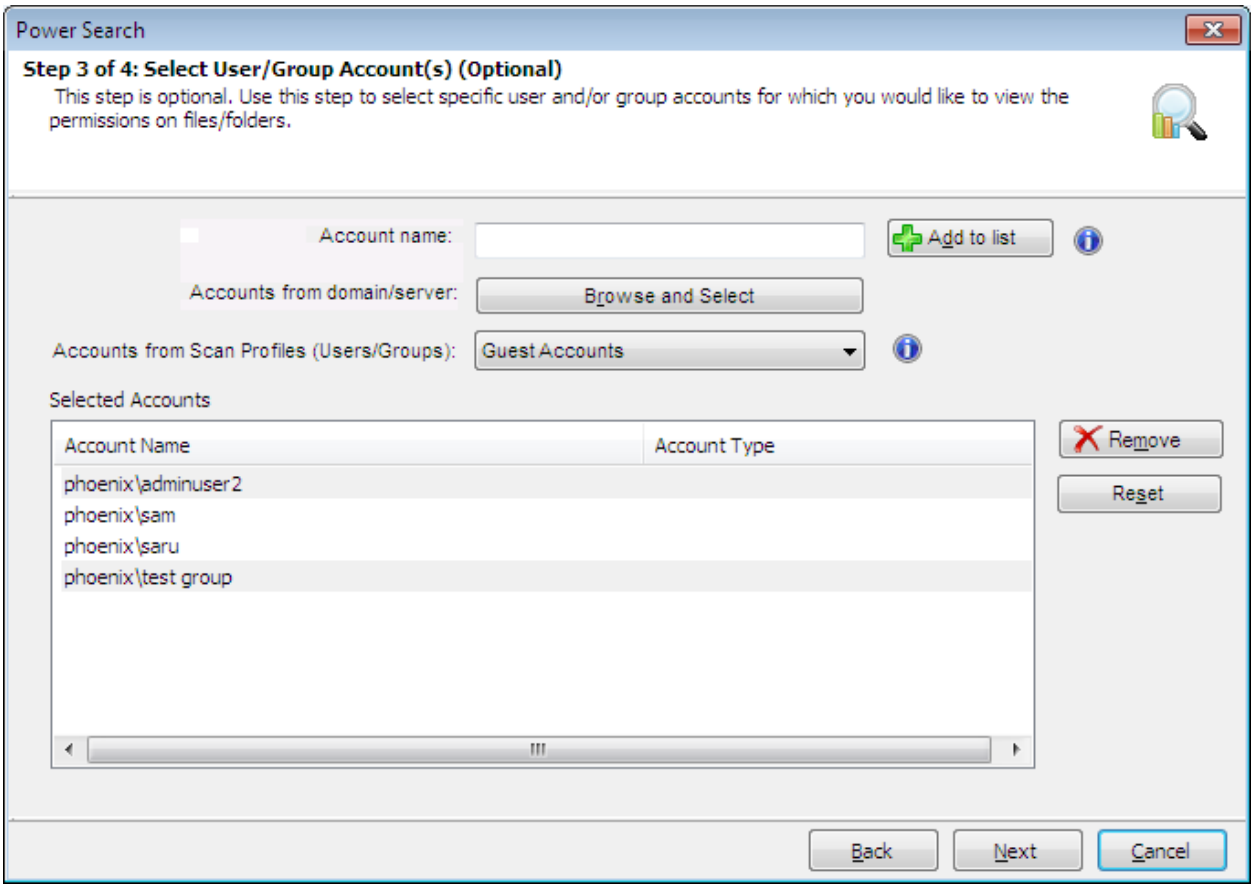


Step 3: User and/or Group Selection

1. Select the user or group, for which you wish to run the search.
2. The selected users will be added to the wizard as shown below:



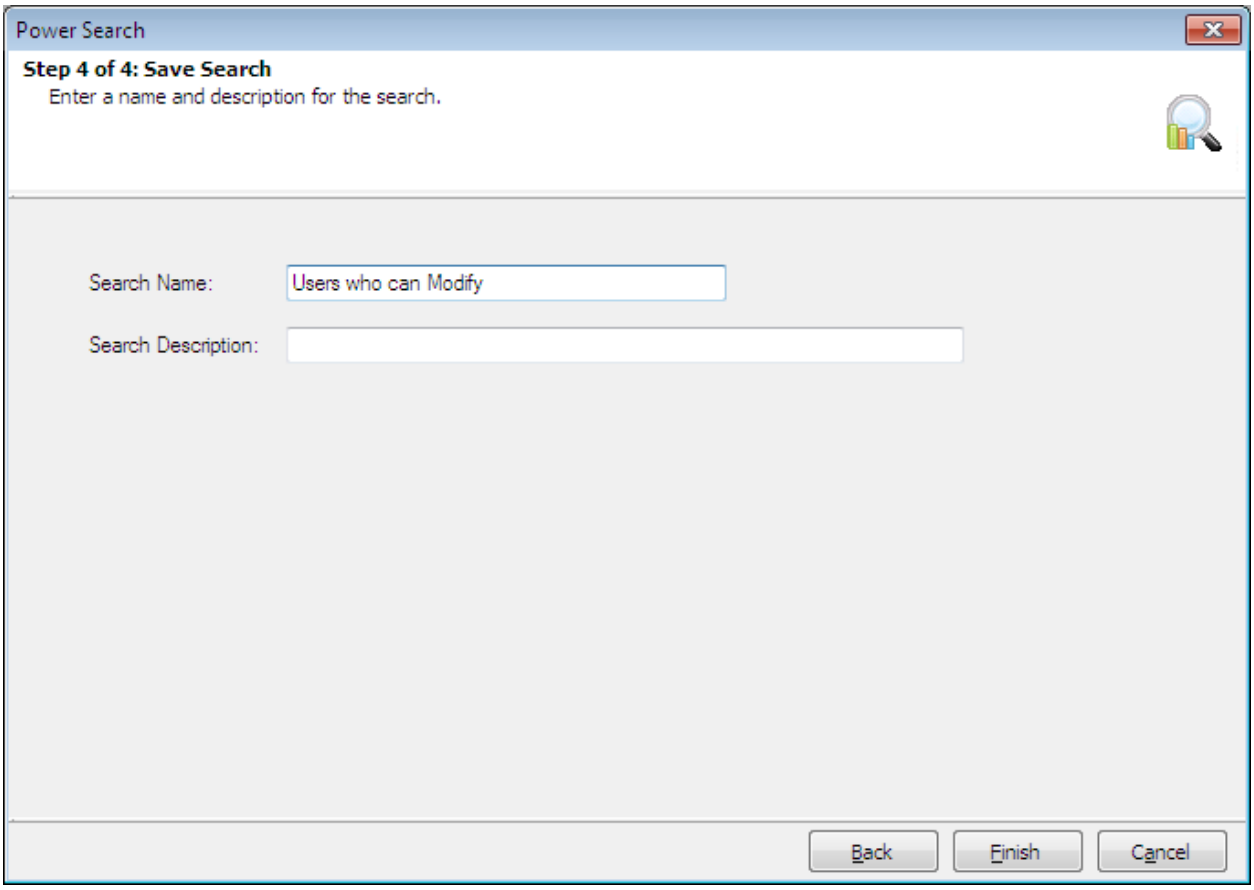
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile.



- Click **Next** to proceed to the Next step.

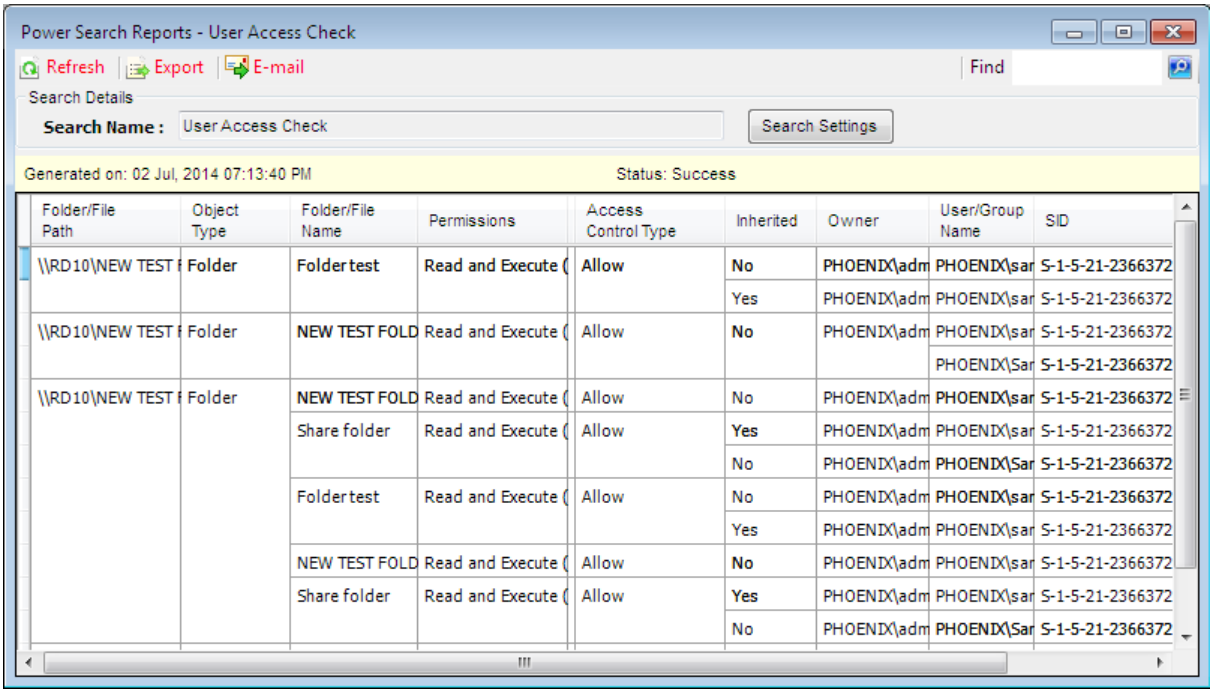
Step 4: Save Search

Enter a name and description for search.



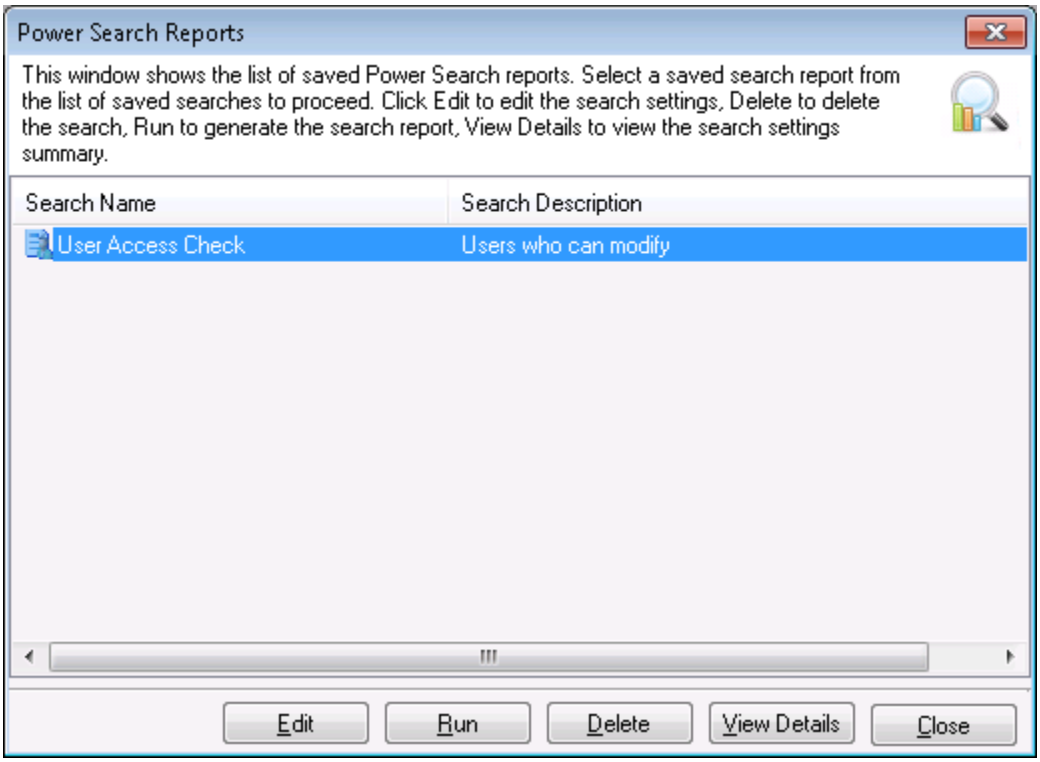
Click **Finish** to generate the power search report.

After the data collection process is complete, the report would be generated in a report window as shown below:


Power Search Reports - User Access Check
Refresh
Export
E-mail
Find
Search Details
Search Name :
User Access Check
Search Settings
Generated on: 02 Jul, 2014 07:13:40 PM
Status: Success
Folder/File Path
Object Type
Folder/File Name
Permissions
Access Control Type
Inherited
Owner
User/Group Name
SID
\\RD10\NEW TEST F
Folder
Folder test
Read and Execute (
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
\\RD10\NEW TEST F
Folder
NEW TEST FOLD
Read and Execute (
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
PHOENIX\Sar
S-1-5-21-2366372
\\RD10\NEW TEST F
Folder
NEW TEST FOLD
Read and Execute (
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Share folder
Read and Execute (
Allow
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
No
PHOENIX\adm
PHOENIX\Sar
S-1-5-21-2366372
Folder test
Read and Execute (
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
NEW TEST FOLD
Read and Execute (
Allow
No
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
Share folder
Read and Execute (
Allow
Yes
PHOENIX\adm
PHOENIX\sar
S-1-5-21-2366372
No
PHOENIX\adm
PHOENIX\Sar
S-1-5-21-2366372

How to manage Power Search?

Click to launch the saved search(s) window. The windows shows the list of search(s) that were saved over the period of time.


Power Search Reports
This window shows the list of saved Power Search reports. Select a saved search report from the list of saved searches to proceed. Click Edit to edit the search settings, Delete to delete the search, Run to generate the search report, View Details to view the search settings summary.
Search Name
Search Description
User Access Check
Users who can modify
Edit
Run
Delete
View Details
Close

The saved search window allows you to perform the following operations:

- Run an existing search
- Edit an existing search
- Delete a search
- Preview the settings of a search

Run an existing search

1. To Run an existing search click **Run** button in the window. The Power Search report window will appear on the screen and the report will be displayed once the data collection is finished.
2. During edit operation you can modify the search inputs, however, you cannot modify the type of the Scan Profile.

Edit an existing search

To edit an existing search click **Edit** button in the window. The Power Search Dialog will appear on the screen which will allow you to edit the selected search.

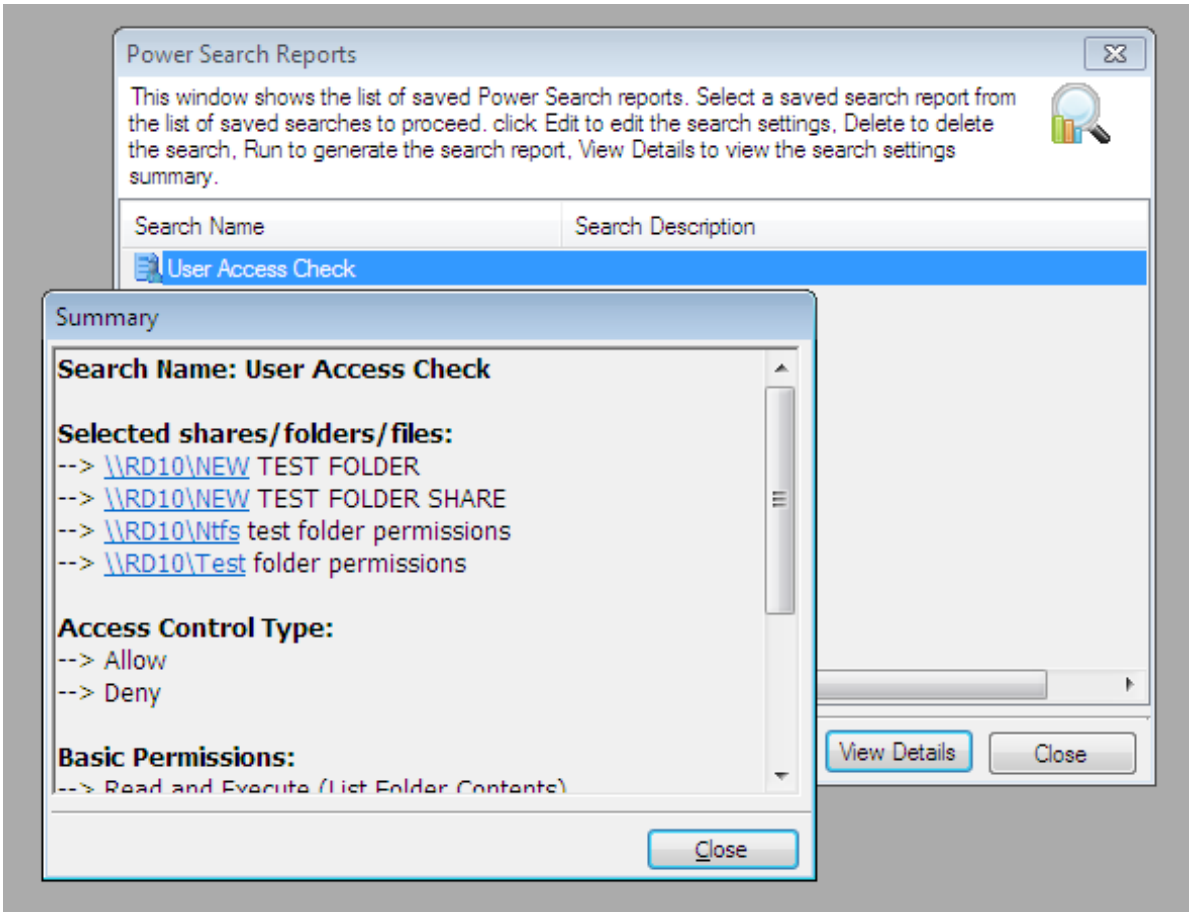
During edit operation you can modify the computer list, however, you cannot modify the name of the search.

Delete a search

To delete a search, select the search you want to delete, and then click **Delete** button. The selected search will be deleted permanently.

Preview the settings of a search

To preview the settings of a saved search, select a search, and then click **View Details** button. The settings will be displayed in a window as shown below:


Power Search Reports
This window shows the list of saved Power Search reports. Select a saved search report from the list of saved searches to proceed. click Edit to edit the search settings, Delete to delete the search, Run to generate the search report, View Details to view the search settings summary.
Search Name
Search Description
User Access Check
Summary
Search Name: User Access Check
Selected shares/folders/files:
--> \\RD10\NEW TEST FOLDER
--> \\RD10\NEW TEST FOLDER SHARE
--> \\RD10\Ntfs test folder permissions
--> \\RD10\Test folder permissions
Access Control Type:
--> Allow
--> Deny
Basic Permissions:
Close
View Details
Close

Change History

About Change History

How to view Permissions Change History?

How to view Central Access Policies Change History?

About Change History

The Change History feature lets you view the Permissions and Central Access Policies change history of NTFS Security Manager with the specified date interval.

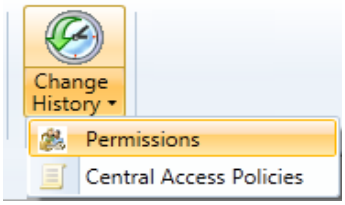
For more information about Change History follow the links given below.

How to view Permissions Change History?

How to view Central Access Policies Change History?

How to view Permissions Change History?

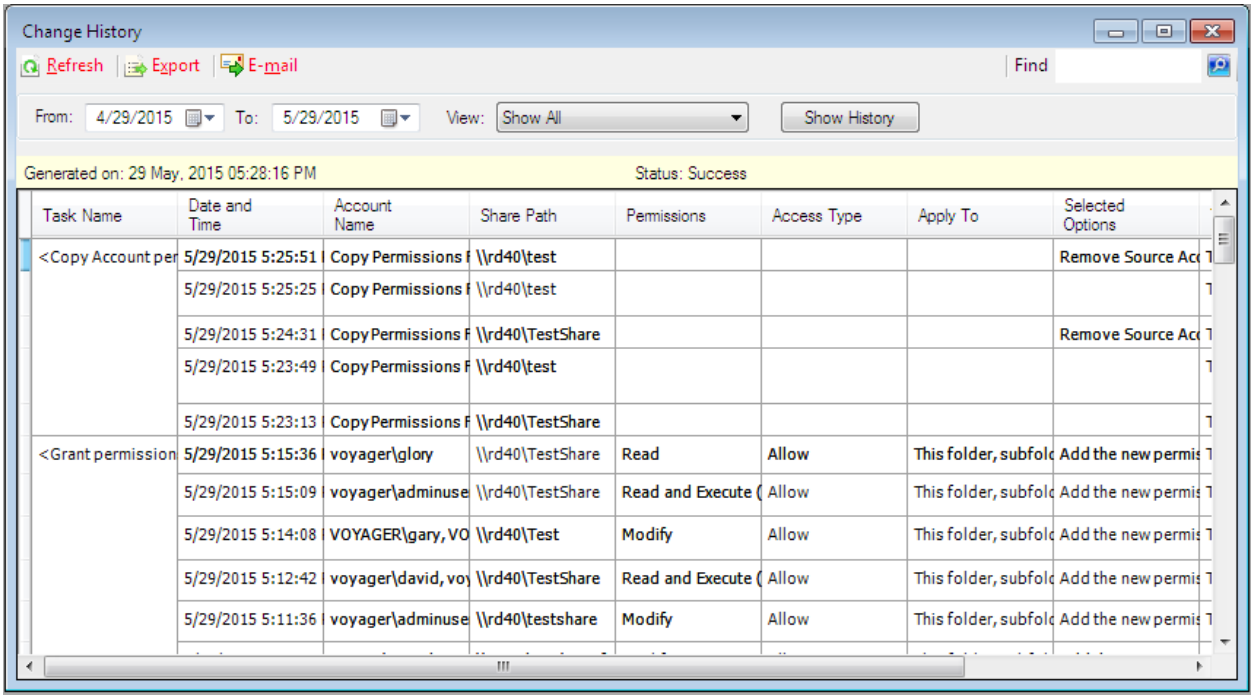
The **Change History** feature allows you to view permissions change history of NTFS Security Manager. You can view permissions change history between specific date interval by selecting From and To dates. By default, it shows the history of last 30 days. You can view permissions change history of specific task by selecting task name in the View option.

Click on 

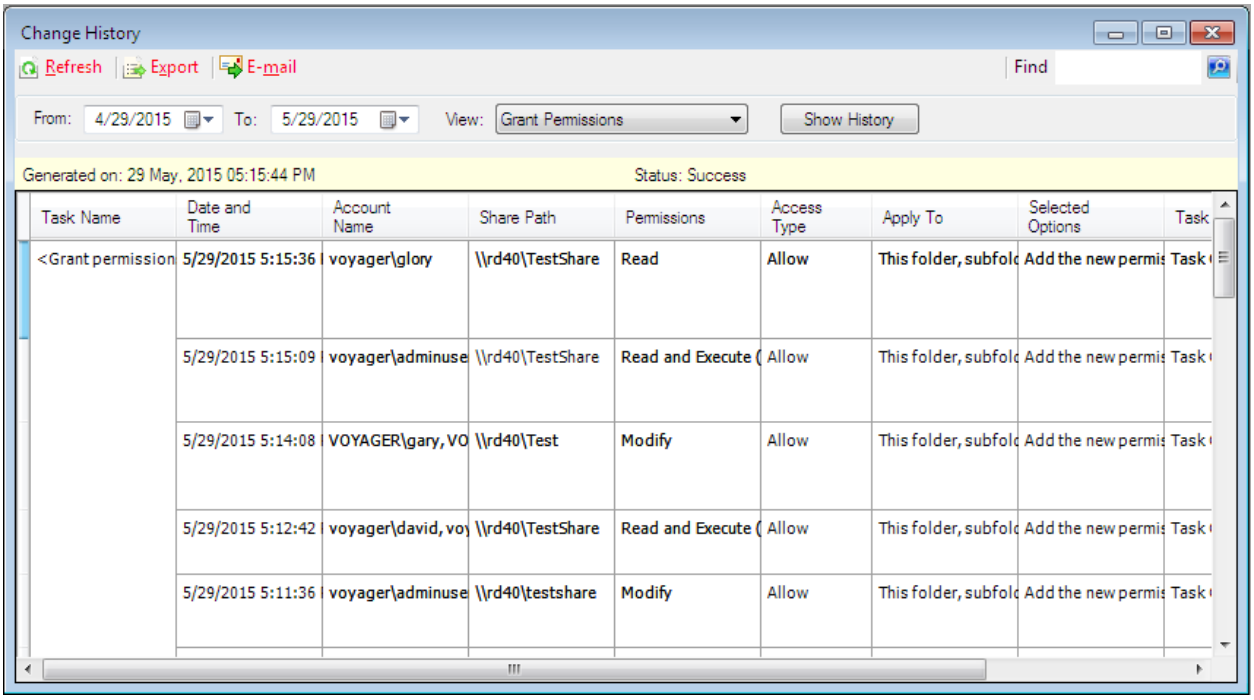
button in the toolbar.

The Change History window will be displayed as shown below. You can view Permissions Change History in one of the following ways.

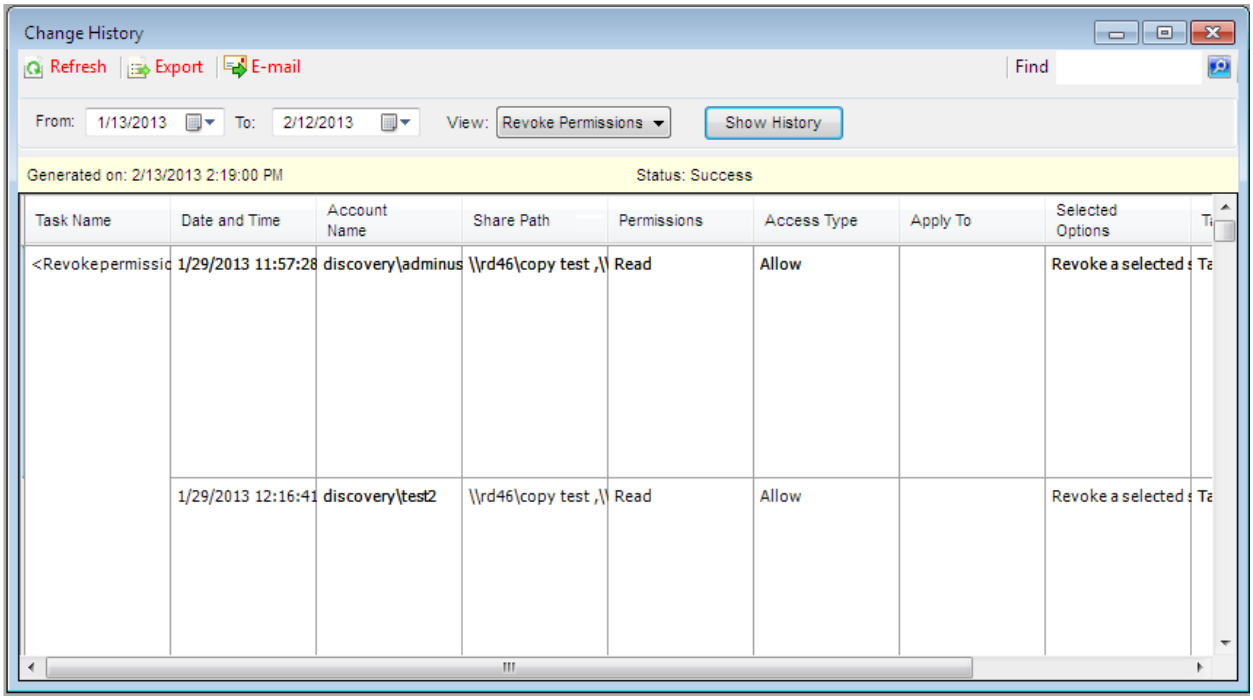
- Grant Permissions History
- Revoke Permissions History
- Copy Permissions History
- Modify Permissions History
- Copy Account Permissions History


Change History
Refresh
Export
E-mail
Find
From: 4/29/2015
To: 5/29/2015
View: Show All
Show History
Generated on: 29 May, 2015 05:28:16 PM
Status: Success
Task Name | Date and Time | Account Name | Share Path | Permissions | Access Type | Apply To | Selected Options
<Copy Account per | 5/29/2015 5:25:51 | Copy Permissions f | \\rd40\test | | | | Remove Source Acc
5/29/2015 5:25:25 | Copy Permissions f | \\rd40\test
5/29/2015 5:24:31 | Copy Permissions F | \\rd40\TestShare | | | | Remove Source Acc
5/29/2015 5:23:49 | Copy Permissions F | \\rd40\test
5/29/2015 5:23:13 | Copy Permissions F | \\rd40\TestShare
<Grant permission | 5/29/2015 5:15:36 | voyager\glory | \\rd40\TestShare | Read | Allow | This folder, subfolc | Add the new permis
5/29/2015 5:15:09 | voyager\adminuse | \\rd40\TestShare | Read and Execute (| Allow | This folder, subfolc | Add the new permis
5/29/2015 5:14:08 | VOYAGER\gary, VO | \\rd40\Test | Modify | Allow | This folder, subfolc | Add the new permis
5/29/2015 5:12:42 | voyager\david, voy | \\rd40\TestShare | Read and Execute (| Allow | This folder, subfolc | Add the new permis
5/29/2015 5:11:36 | voyager\adminuse | \\rd40\testshare | Modify | Allow | This folder, subfolc | Add the new permis

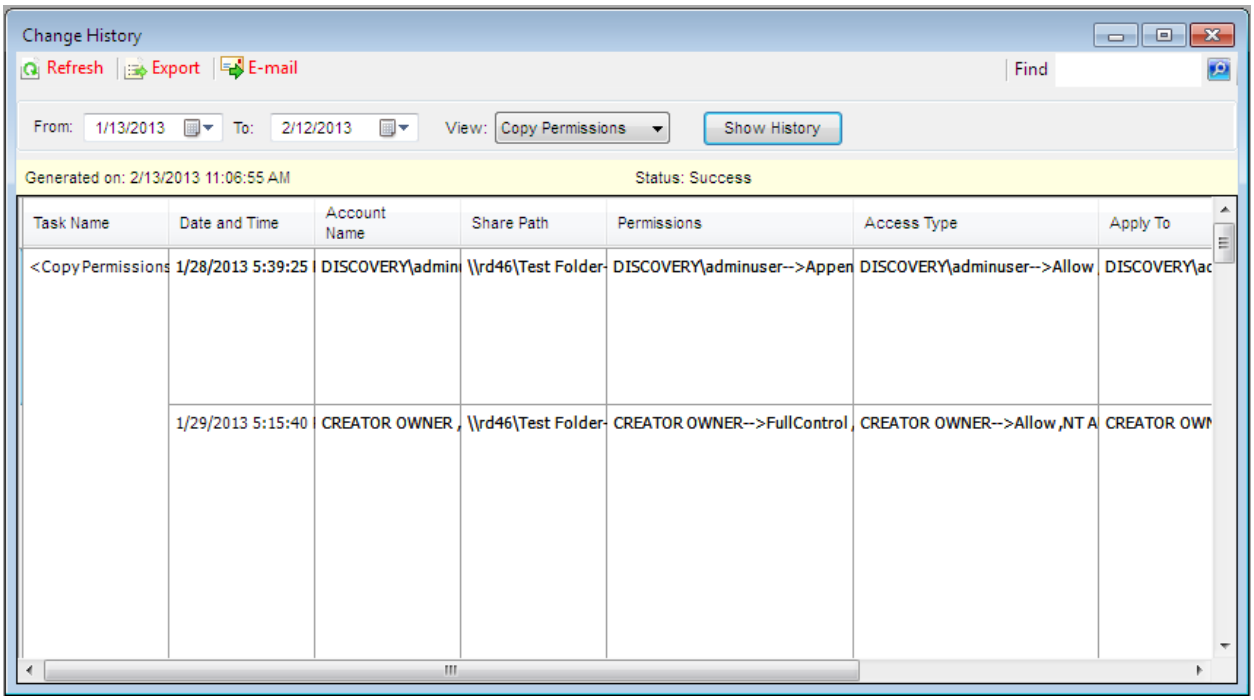
Select required From and To dates. Select **Grant Permissions** in the View option. Then click Show History button. The Grant Permissions history will be displayed as shown below.



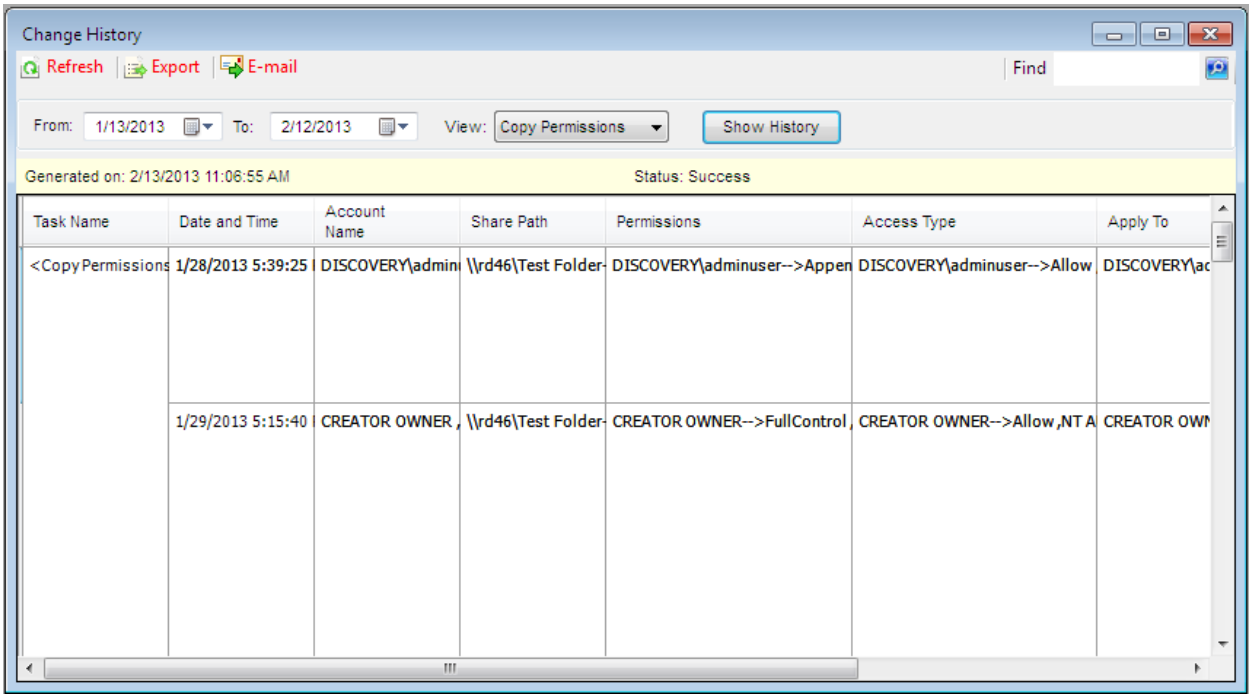
Select required From and To dates. Select **Revoke Permissions** in the View option. Then click Show History button. The Revoke Permissions history will be displayed as shown below.



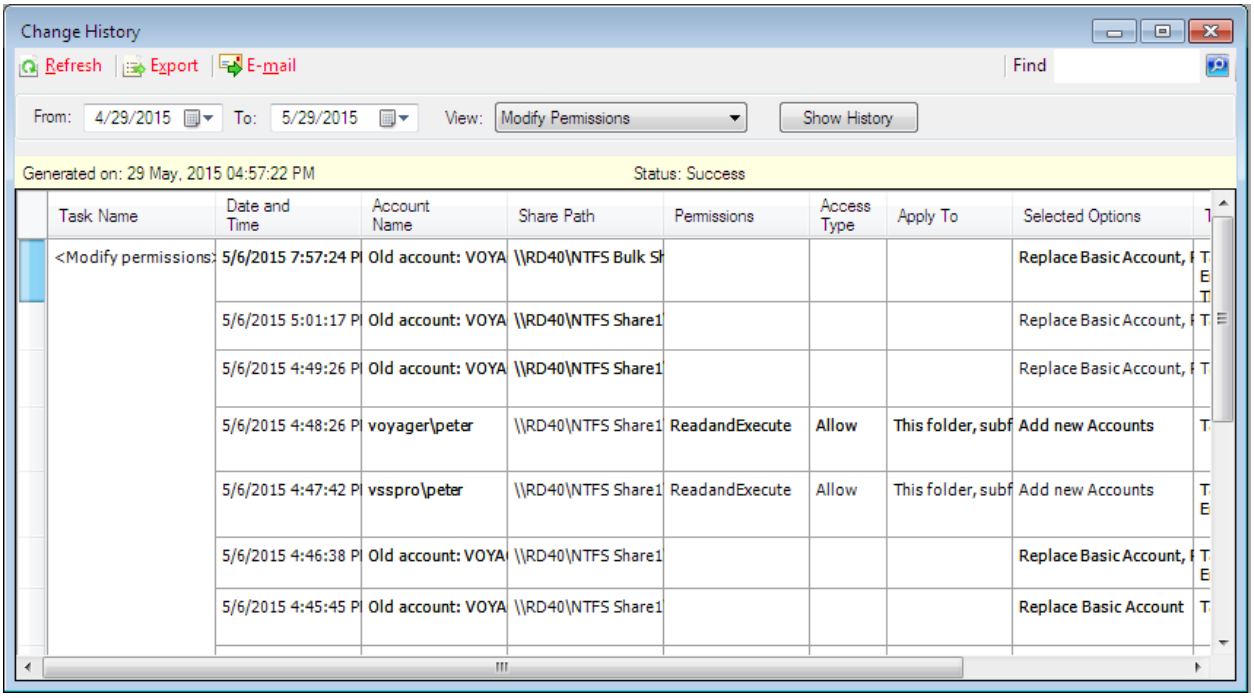
Select required From and To dates. Select **Copy Permissions** in the View option. Then click Show History button. The Copy Permissions history will be displayed as shown below.



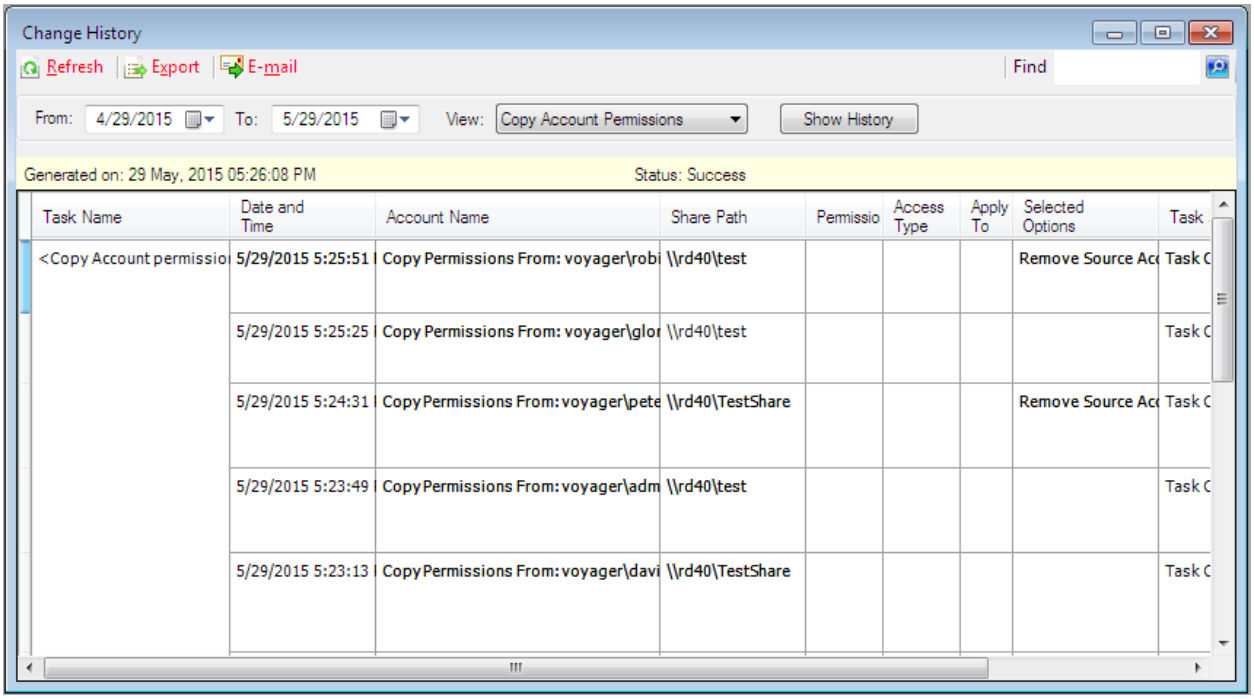
Select required From and To dates. Select **Copy Permissions** in the View option. Then click Show History button. The Replace Permissions history will be displayed as shown below.



Select required From and To dates. Select **Modify Permissions** in the View option. Then click Show History button. The Modify Permissions history will be displayed as shown below:

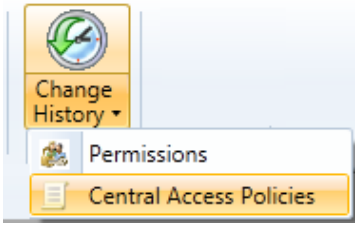


Select required From and To dates. Select **Copy Account Permissions** in the View option. Then click Show History button. The Copy Account Permissions history will be displayed as shown below:



How to view Central Access Policies Change History?

The **Change History** feature allows you to view central access policies change history of NTFS Security Manager. You can view central access policies change history between specific date interval by selecting From and To dates. By default, it shows the history of last 30 days. You can view permissions change history of specific task by selecting task name in the View option.

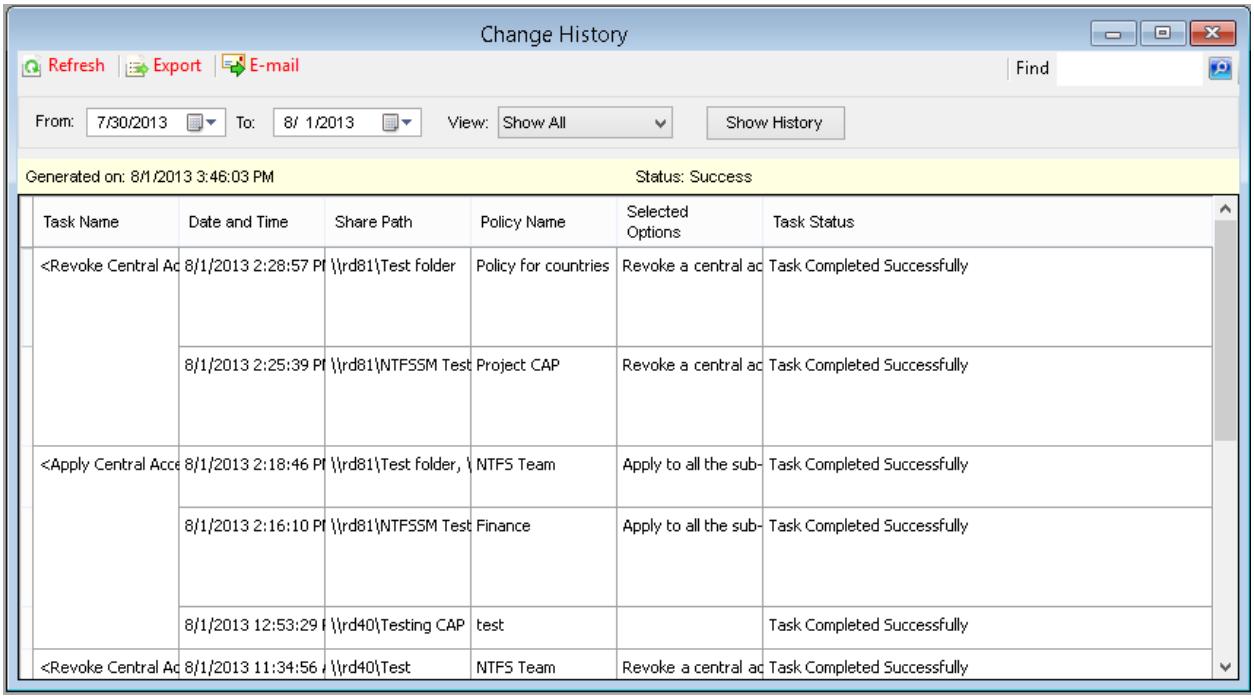
Click on 

button in the toolbar.

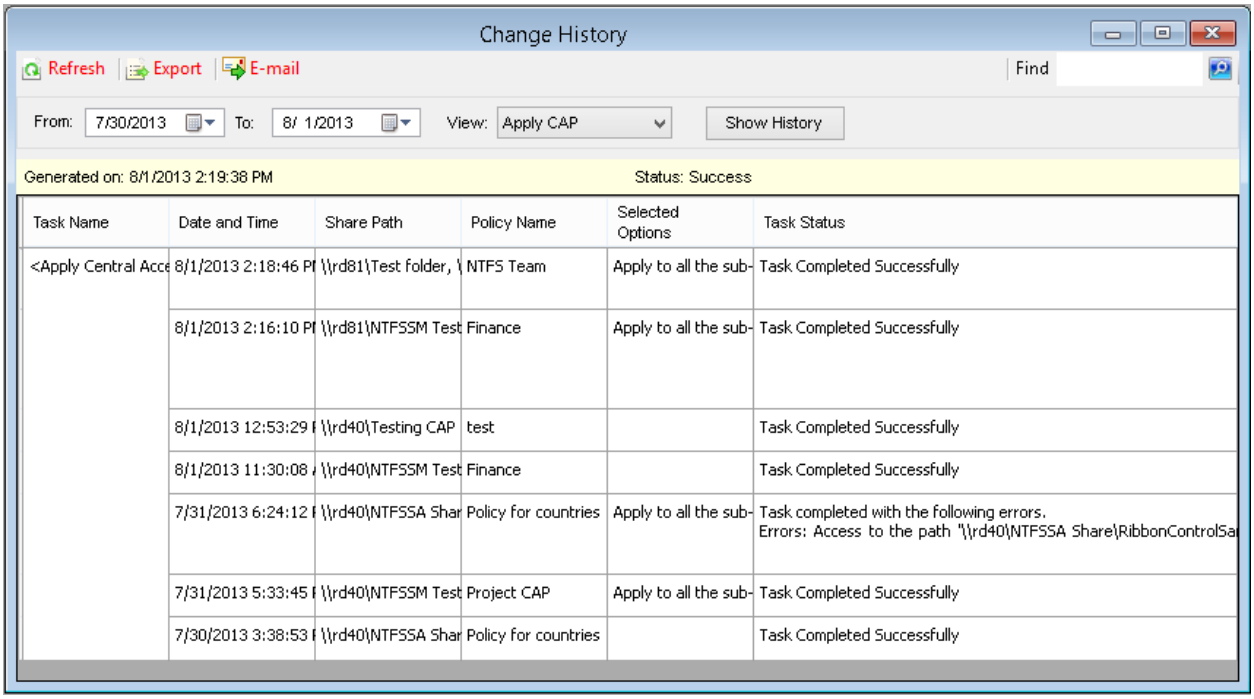
The Central Access Policies Change History window will be displayed as shown below. You can view Central Access Policies Change History in one of the following ways.

Apply CAP History

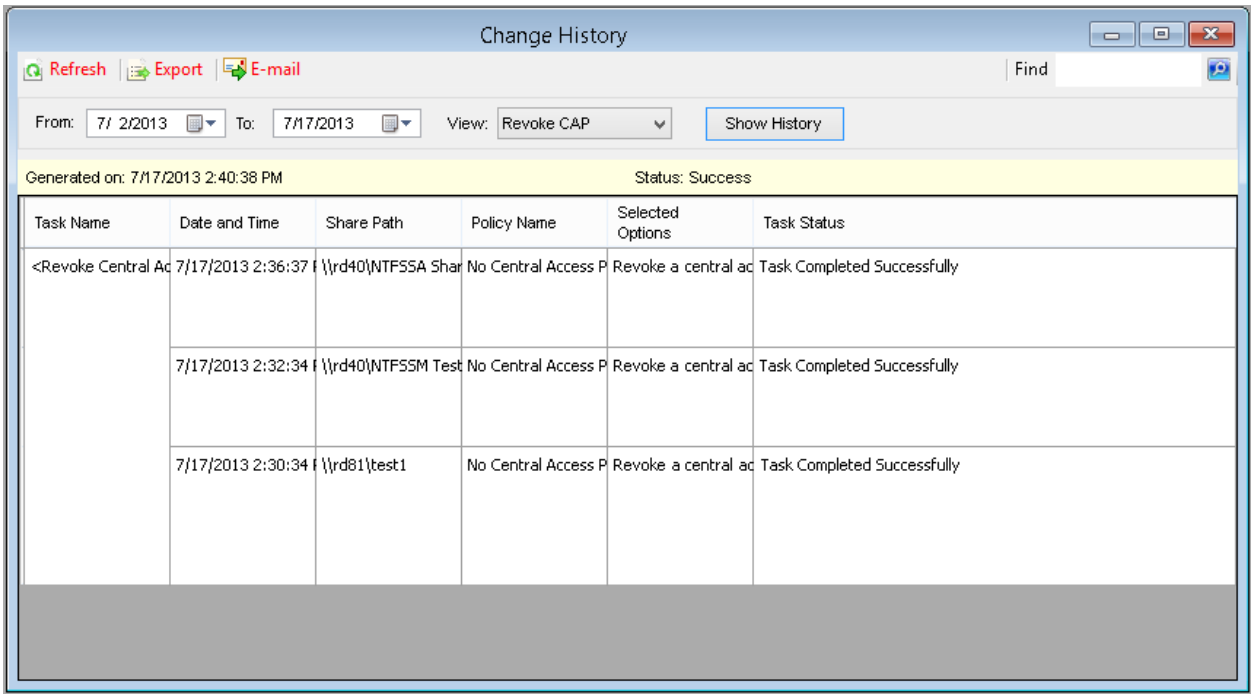
Revoke CAP History



Select required From and To dates. Select **Apply CAP** in the View option. Then click Show History button. The Apply CAP history will be displayed as shown below.



Select required From and To dates. Select **Revoke CAP** in the View option. Then click Show History button. The Revoke CAP history will be displayed as shown below.



Additional Features

How to Customize Fields?

How to Apply Filters?

How to Refresh Data?

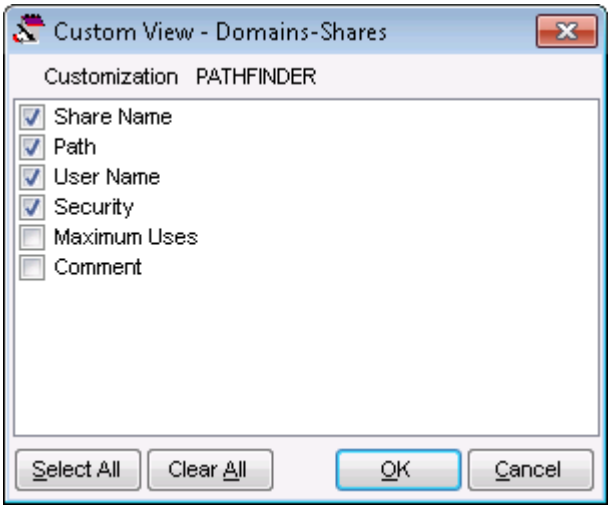
How to Export Data?

How to Email Data?

How to find data in a report?

How to customize fields?

Click on Customize in Standard Reports for customizing the information.



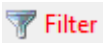
Click Select All for selecting all the check boxes.

Click Clear All for clearing all the check boxes.

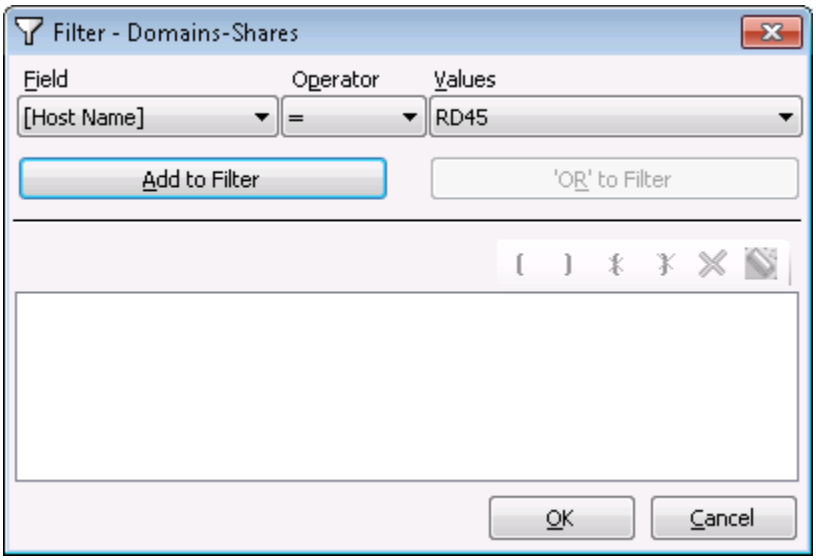
Click OK button for confirming the changes.

Click Cancel button for canceling the operation.

How to Apply Filter?

Click  in Standard Reports for setting filter options.

The **Filter** window will be displayed.



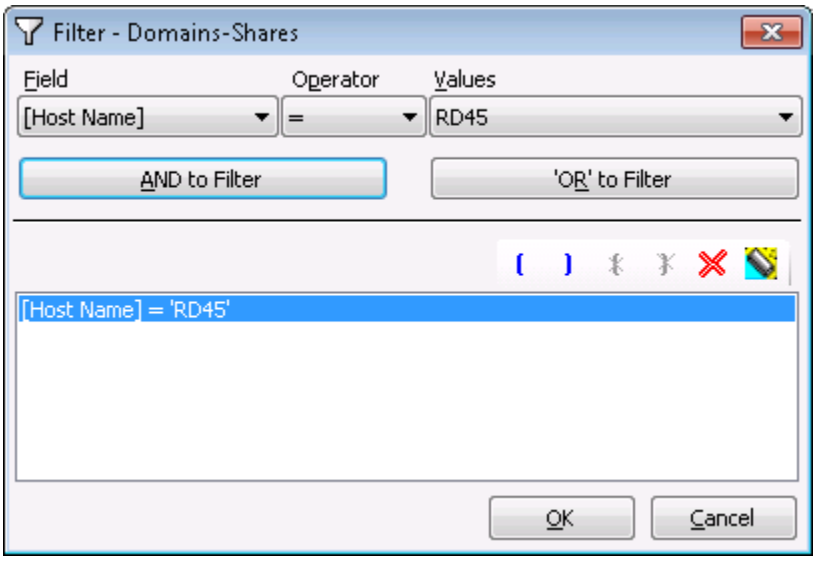
To set a filter condition, follow these steps.

1. Click (Clear All) button and clear the filter.

2. Choose a field name, an operator and a possible value from the respective dropdown options.

3. Click

4. The **Add to Filter** will change to **AND to Filter**. The **OR to Filter** button will be enabled. The selected condition will be set as a filter and displayed (as shown below).



5. Click OK to apply the filter.

Note:

- Use the AND to Filter, 'OR' to Filter and [ ] to build enhanced filter condition as shown below:
- (Field A = Value 1 AND Field B = Value 2) OR (Field C = Value 3 AND Field D = Value 4)
- Use { } to remove the parenthesis
- Use to delete a selected condition.

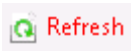
The status bar's **FILTERED** indicator is used to indicate whether the current data is filtered or not.

For a normal view, the status bar will appear as

For a filtered view, the status bar will appear as

How to Refresh data?

Refresh the current report data to view the latest information from the Domain Controller.

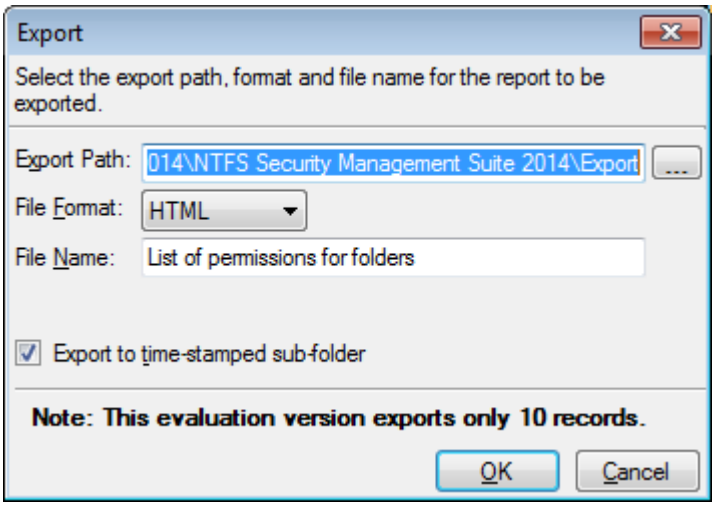
Click on 

button in the toolbar available in the report window or press F5 to refresh report data. Alternatively, you can right-click on the grid, in the right pane of the report window, and then select 'Refresh Data' from the context menu. The existing data will be cleared and latest data will be loaded in the report window.

How to Export data?

The Export feature helps the user to export report data generated by NTFS Security Management Suite to a file using various formats namely HTML/CSV/XLSX/SQL.

Click Export for exporting the information in the desired format.



Specify a file name to export report data to or accept the default file name. Specify the export path and select a desired file format. The path refers to the destination location where the output file generated should be stored. It can be given using the Browse button. To avoid overwrite existing files, if any, in the specified export path, By default, the report will be exported to a time-stamped sub-folder, in the format 'YYYY-MM-DD HH.MM.SS', under the specified export path.

In XLSX file format, the information is stored as sheets in Excel file. For each report, a XLSX file will be generated. The name of the XLSX file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared. The XLSX file will be stored under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path, if "Export to time-stamped folder" option is set.

In CSV file format, the information is stored as comma separated values. For each report, a CSV file will be generated. The name of the CSV file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

In SQL table format, the information is stored as SQL tables in the application database in the specified SQL server based on the selected SQL database option. For each report, a separate table will be created. The name of the table will be the name of the report.

In HTML and XLSX file format, the information is stored in the html and xlsx file respectively. For each report, a HTML file will be generated. The name of the HTML file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a

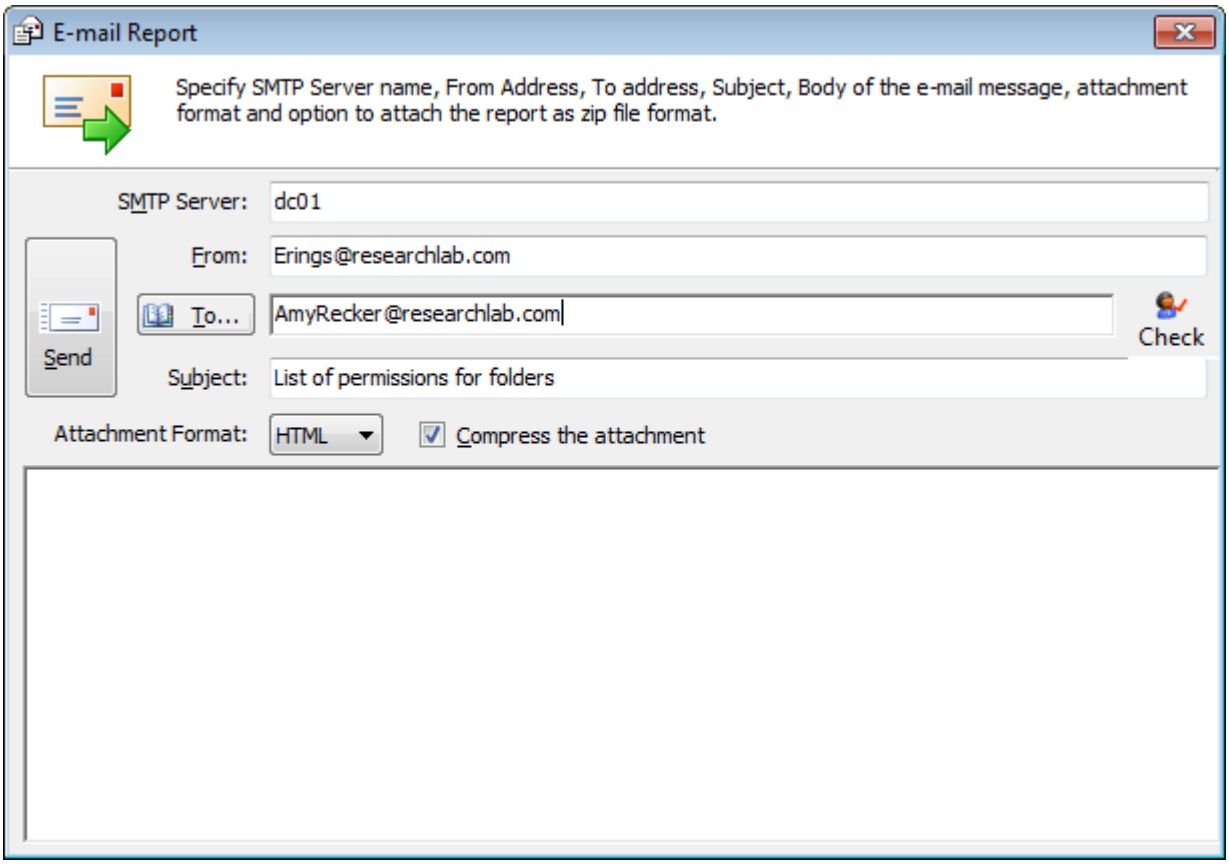
sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

How to E-mail data?

NTFS Security Management Suite provides the option to e-mail the reports generated.

Click

button in the toolbar to e-mail the report to e-mail recipients. E-mail dialog will be displayed as shown below:



For e-mailing reports, NTFS Security Management Suite requires SMTP Server, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the report attachment format.

Specify SMTP server name, from Address, To address, mail subject, mail content, attachment format and option to compress the attachment.

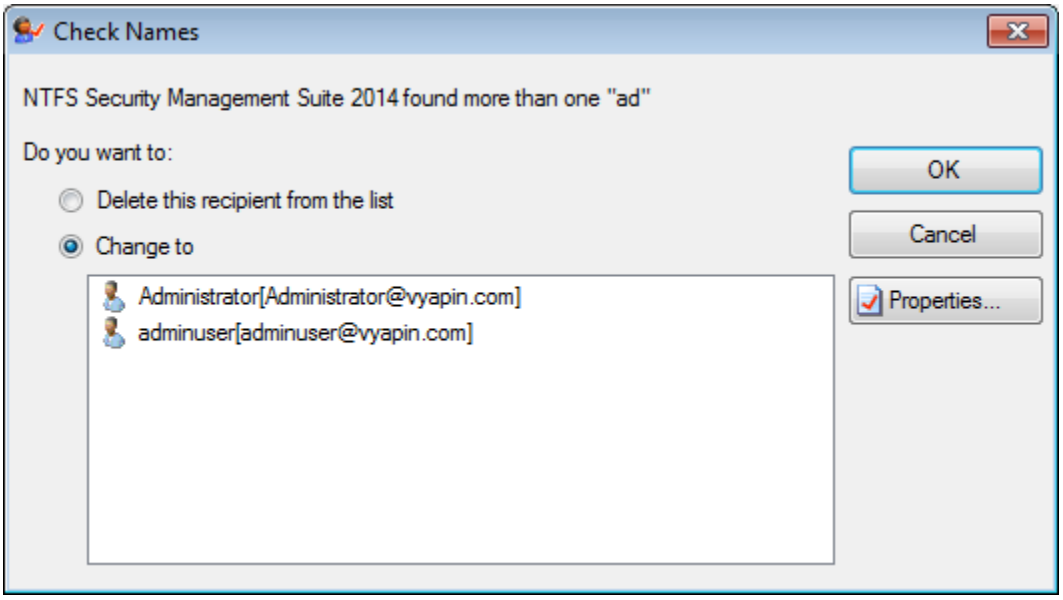
Click

button to send the report by e-mail to the selected recipients.

Check names

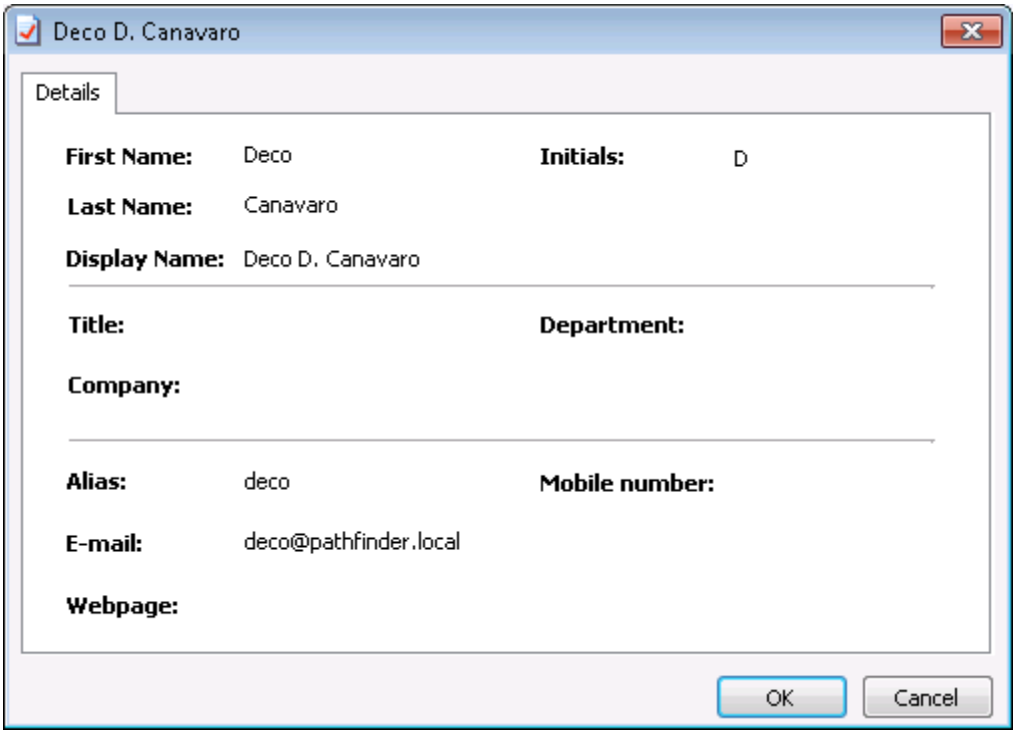
NTFS Security Management Suite provides check name feature to check the existence of corresponding mail-enabled recipient object in Active Directory. To check name, click

button. If the entered name matches with a mail object in the Active directory / its trusted domain, name entered in From address textbox will be replaced by the corresponding active directory recipient object. If there is more than one match, a dialog which contains matching Active Directory recipients will appear as shown below. You can select one or more recipient and click **OK**.

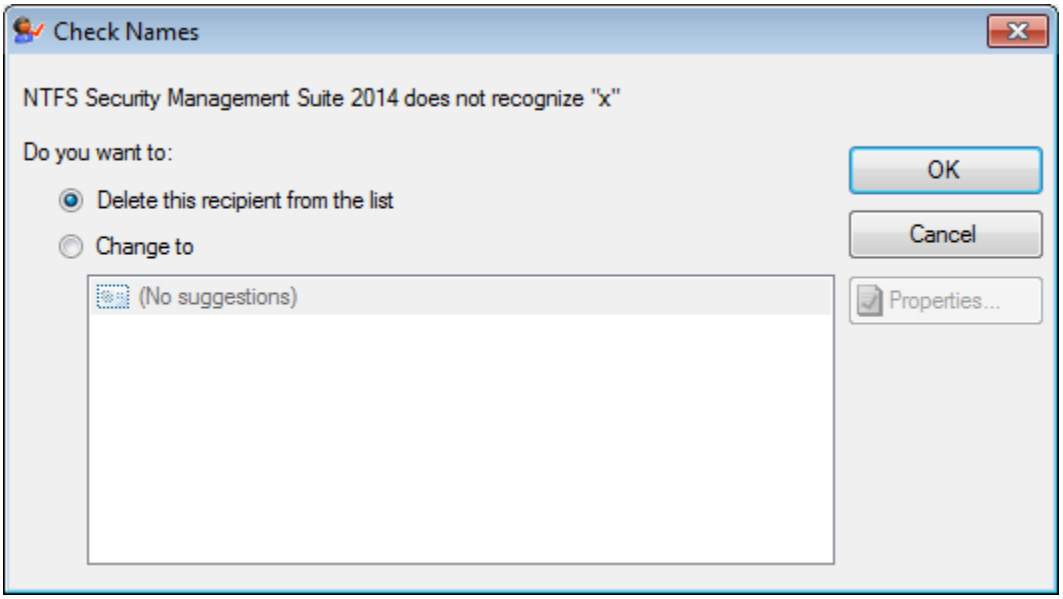


To get more information about the listed recipients under Change to, select the name, and then click

.

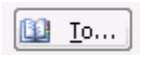


If there is no match for the name entered by the user in Active Directory, a dialog will appear as shown below:

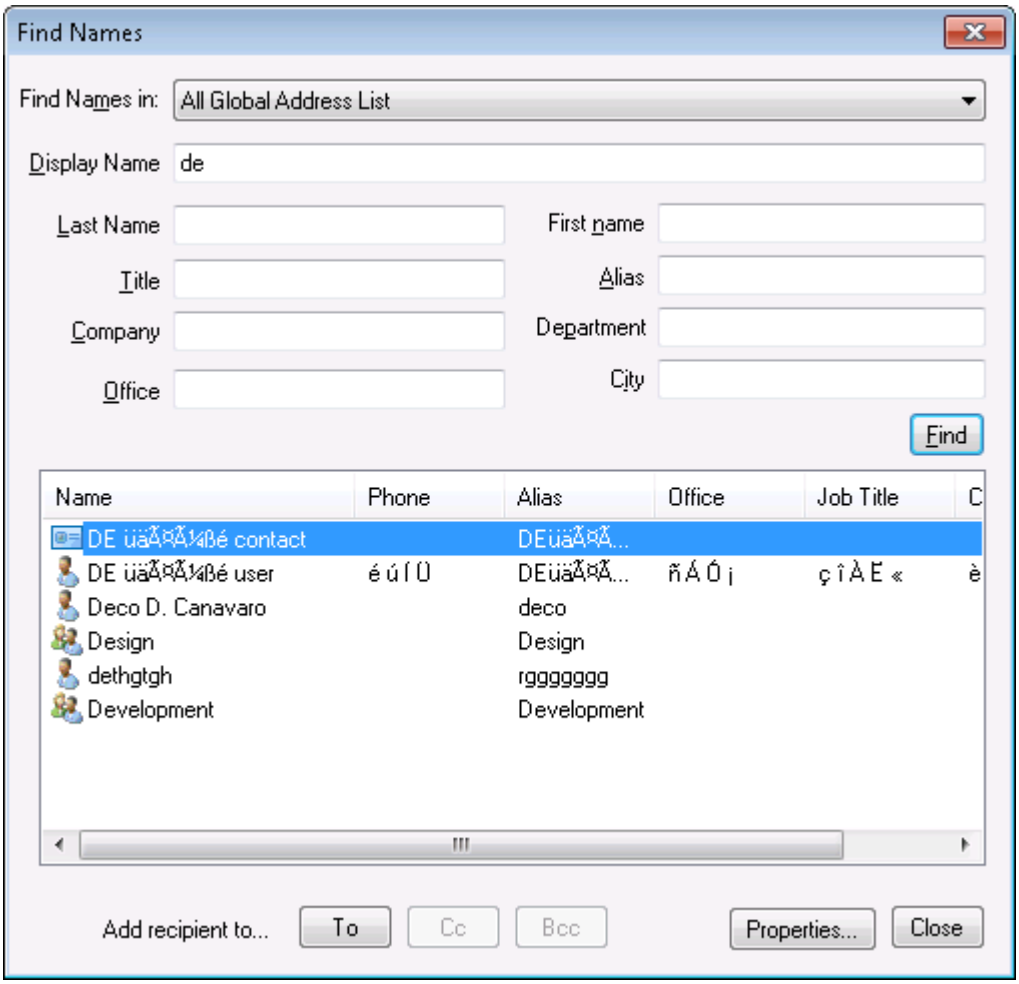


Select Delete option in the above dialog to remove the recipient name from To address text box. Click Cancel button to close this dialog and the unresolved recipient(s) will appear in red color.

Address Book

NTFS Security Management Suite provides Address Book feature to search for any mail enabled recipient object (say, person, distribution list, contact, public folder) you want to send a message to. Click 

button and then use the **Find Names** dialog box to search for the recipient object you want to send a message to. (Note that you can't use the **Find Names** dialog box to search for distribution lists in your Contacts folder.) Select the object's name in the list and then click **Add recipient to...**.

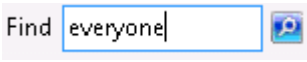


To get more information about one of the names in the list, such as department or phone number, select the name, and then click

.

How to find data in a report?

You can use the find feature in NTFS Security Management Suite to search for specific data in a report.

To search for data in a report, just type the characters or words you want to find in the find edit box available in the report window and click on 

.

1. NTFS Security Management Suite performs a case insensitive search of the specified search criteria in the report.

2. The search criteria should not be enclosed within quotation marks.

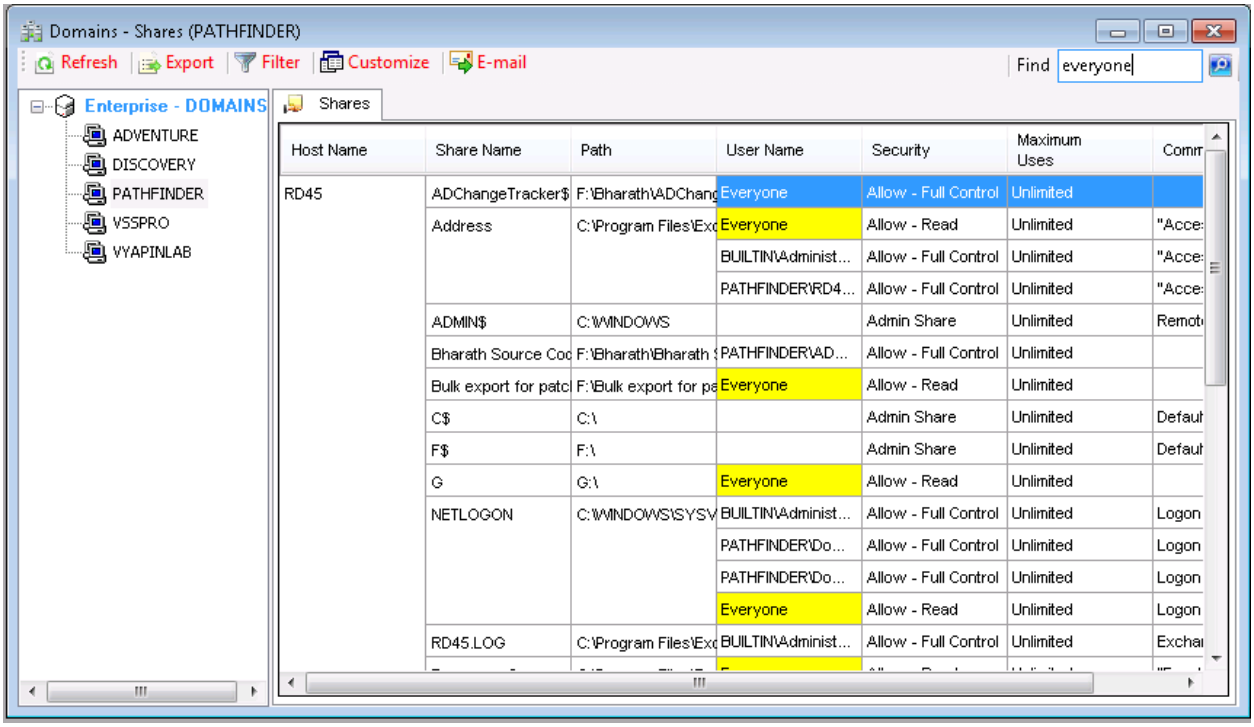
3. You can use the "*" wildcard character in the search criteria. The "*" wildcard character act as a place holder for zero or more characters. However, note that you cannot use the "?" wildcard character in the search criteria.

For instance, if you want to search for 'Domain' in a report. Type Domain, without quotations, in the edit box, and then click on Find Button.

By default, NTFS Security Management Suite adds an asterisk as a suffix to the specified search criteria, if no wildcard character is present in it. In this case, NTFS Security Management Suite finds a match in the report for all fields that have the text Domain followed by zero or more characters, that is, Domain, Domain Controllers, Domain Admins, etc.

For all the matches found, NTFS Security Management Suite highlights the corresponding columns in the grid, and scrolls the grid automatically to the first occurrence.

4. NTFS Security Management Suite finds additional occurrences of the specified search criteria instantaneously. To locate other occurrences of the same search criteria in a report you need to scroll the report grid downwards.


Domains - Shares (PATHFINDER)
Refresh
Export
Filter
Customize
E-mail
Find
everyone
Enterprise - DOMAINS
ADVENTURE
DISCOVERY
PATHFINDER
VSSPRO
VYAPINLAB
Shares
Host Name
Share Name
Path
User Name
Security
Maximum Uses
RD45
ADChangeTracker$
Everyone
Allow - Full Control
Unlimited
Address
Allow - Read
BUILTIN\Administ...
PATHFINDER\RD4...
ADMIN$
C:\WINDOWS
Admin Share
Bharath Source Coc
PATHFINDER\AD...
Bulk export for patcl
C$
C:\
F$
F:\
G
G:\
NETLOGON
PATHFINDER\Do...
RD45.LOG

Scan Profiles Manager

About Scan Profiles (Computers)

How to create Scan Profiles (Computers)?

How to manage Scan Profiles (Computers)?

How to apply Scan Profiles (Computers) in NTFS Security Auditor Module?

How to apply Scan Profiles (Computers) in NTFS Security Manager Module?

About Scan Profiles (Users / Groups)

How to create Scan Profiles (Users / Groups)?

How to manage Scan Profiles (Users / Groups)?

How to apply Scan Profiles (Users / Groups) in NTFS Security Auditor Module?

How to apply Scan Profiles in (Users / Groups) in NTFS Security Manager Module?

About Scan Profiles (Shares)

How to create Scan Profiles (Shares)?

How to manage Scan Profiles (Shares)?

How to apply Scan Profiles (Shares) in NTFS Security Auditor Module?

How to apply Scan Profiles (Shares) in NTFS Security Manager Module?

About Scan Profiles (Computers)

You can setup Scan Profiles to scan a subset of computers in the network and save these profiles for repeated use while generating reports (useful for repeatedly scanning and reporting on different subsets of computers).

You can create Scan Profiles in one of the following ways:

- Selecting specific computers in the network
- Selecting specific Windows versions
- Importing list of computers from a text file
- Importing list of IP addresses from a text file

For more information about Scan Profiles follow the links given below.

- How to create Scan Profiles (Computers)?
- How to manage Scan Profiles (Computers)?
- How to apply Scan Profiles (Computers)?

How to create Scan Profiles (Computers)?

The Scan Profile Dialog allows you to create or edit a Scan Profile. During edit operation, the name of a Scan Profile and its type cannot be modified. You can access the Scan Profile Dialog from the Scan Profiles Manager.

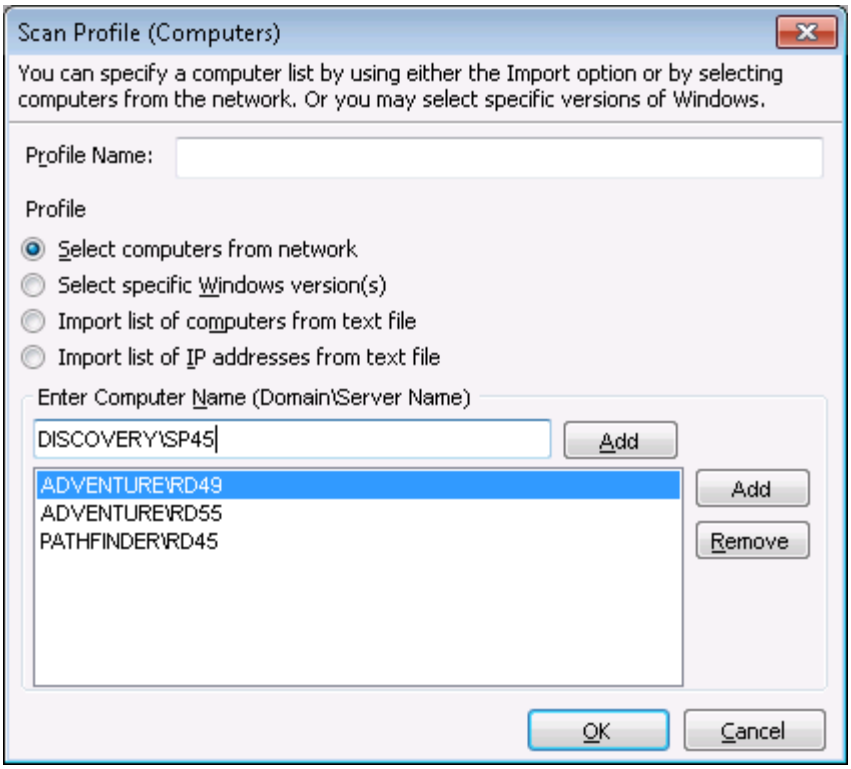
Perform the following steps to create a Scan Profile.

1. Click **New** button in the Scan Profiles Manager window. The Scan Profile dialog will show up on screen.

2. Specify a name for the Scan Profile. You must give a unique name for the Scan Profile.

3. Specify how you want to create the profile by selecting appropriate profile type. You can create Scan Profiles in one of the following ways:

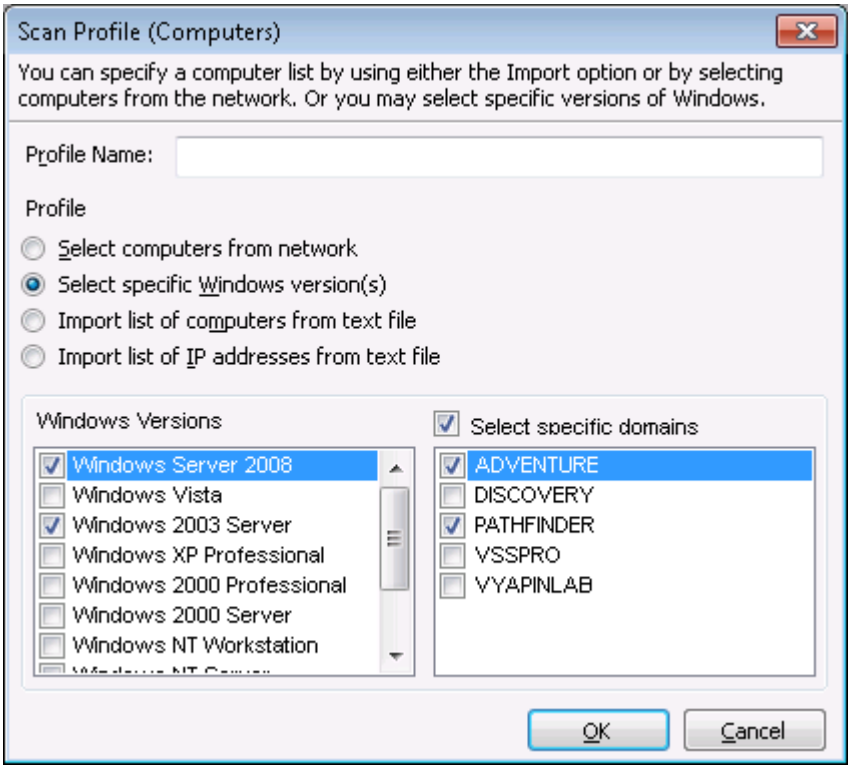
A. Selecting computers from network



I. Select **Select computers from network** option.

II. You can type in computer name, in the format "Domain Name\Computer Name", and then click **Add** button to manually add it to the list. Or you may click **Add From** button to browse the network and select specific computers.

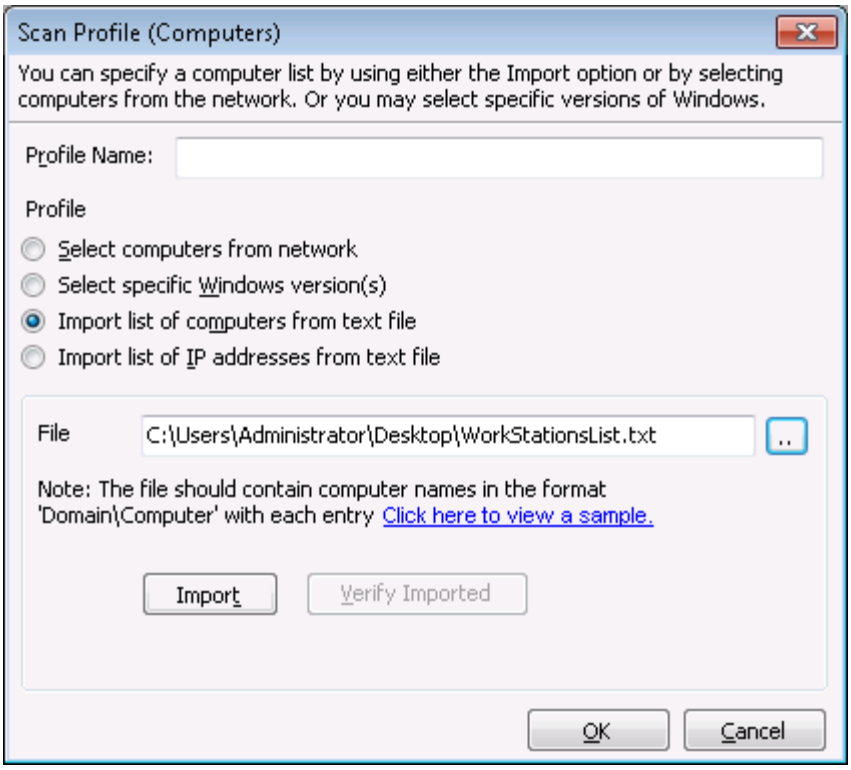
B. Selecting specific Windows versions



i. Select **Select specific Windows version(s)** option.
ii. Select one or more Windows versions. Only computers running the selected Windows version will be included in the computer list.
iii. You may optionally select specific domains, from the list of domains, to include computers only from the selected domains. If you choose not to select any domains, then the Scan Profile includes all domains in the network.

Note: This type of profile is dynamic in nature, in that the list of computers are prepared at run-time; that is at report generation time.

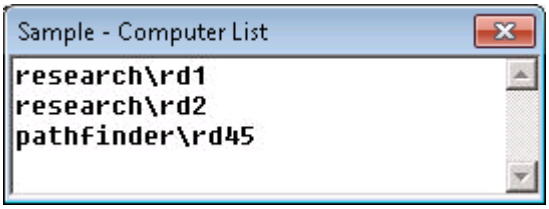
C. Importing list of computers from a text file


Scan Profile (Computers)
You can specify a computer list by using either the Import option or by selecting computers from the network. Or you may select specific versions of Windows.
Profile Name:
Profile
Select computers from network
Select specific Windows version(s)
Import list of computers from text file
Import list of IP addresses from text file
File
C:\Users\Administrator\Desktop\WorkStationsList.txt
..
Note: The file should contain computer names in the format 'Domain\Computer' with each entry Click here to view a sample.
Import
Verify Imported
OK
Cancel

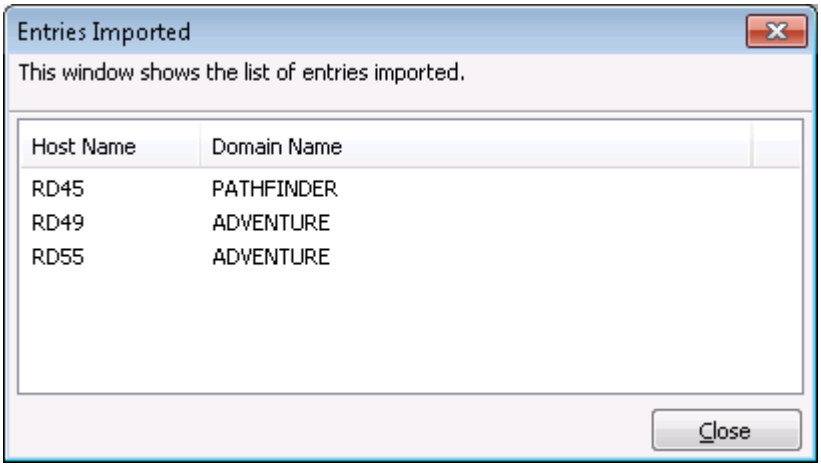
i. Select Import list of computers from text file option.
ii. Click browse ("...") button to select a file that contains the list of computers to be imported.
iii. In the "Select File" dialog that shows up, select a text (.txt) file, and then click Open.
iv. Click Import button to import the list of computers from the selected file.

Note:

- The text file should contain computer names in the format "Domain Name\Computer Name" (both Domain and Computer name should be a NETBIOS name) with each entry in a separate line as shown below:

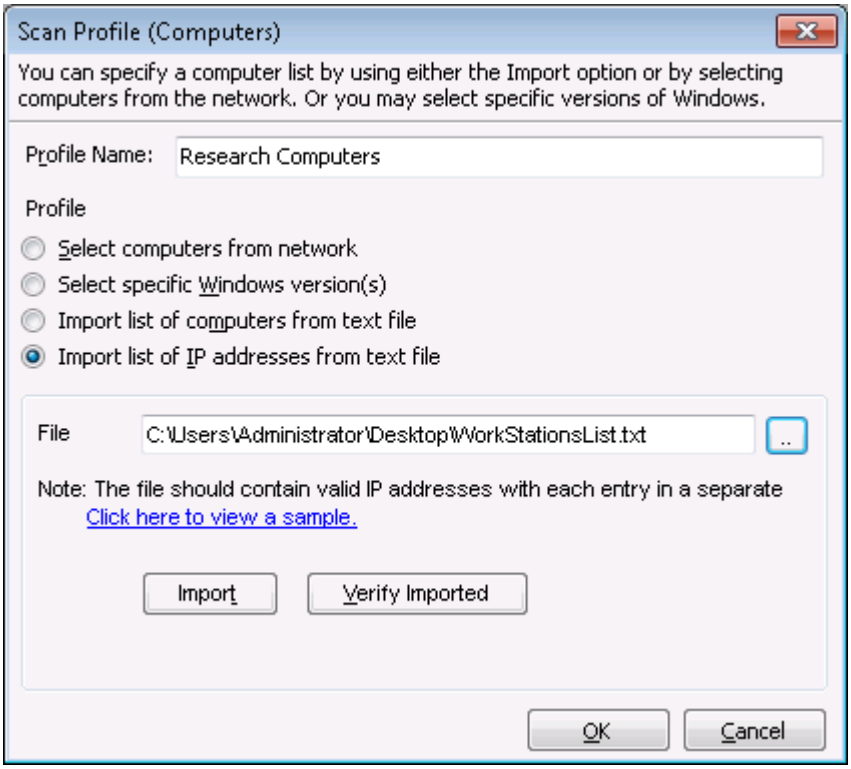


- Only valid entries of the form "Domain Name\Computer Name" will be imported, and invalid entries will be ignored. Please note that the domain specified will be matched with the domain name to which the computer belongs. The computer entry will be ignored either if the domain name does not match or an if error occurs retrieving the domain name. To view the list of entries imported, click Verify Imported List button. The list of computer names imported will be displayed as shown below:



- Changes to the external text file will not automatically be reflected in the Scan Profile. You need to edit the Scan Profile and re-import the updated computer list from the file.

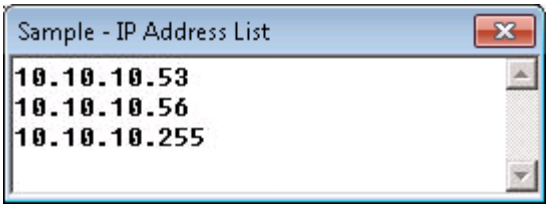
D. Importing list of IP addresses from a text file


Scan Profile (Computers)
You can specify a computer list by using either the Import option or by selecting computers from the network. Or you may select specific versions of Windows.
Profile Name:
Research Computers
Profile
Select computers from network
Select specific Windows version(s)
Import list of computers from text file
Import list of IP addresses from text file
File
C:\Users\Administrator\Desktop\WorkStationsList.txt
..
Note: The file should contain valid IP addresses with each entry in a separate
Click here to view a sample.
Import
Verify Imported
OK
Cancel

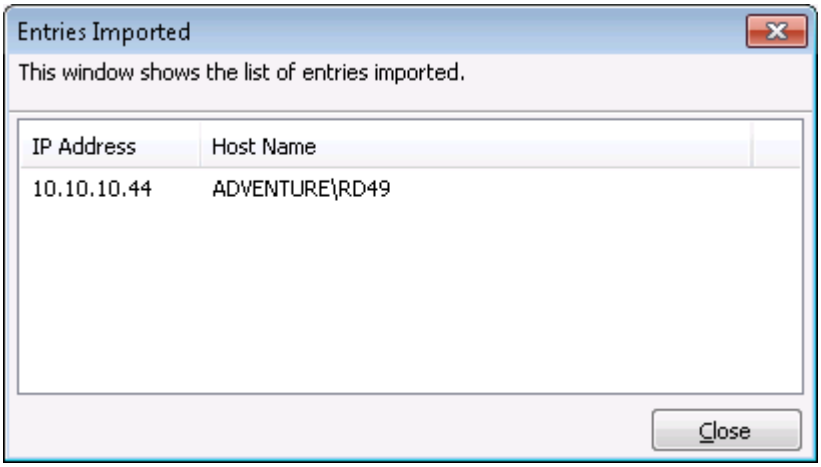
i. Select **Import list of IP addresses from text file** option.
ii. Click browse ("...") button to select a file that contains the list of IP addresses to be imported.
iii. In the "Select File" dialog that shows up, select a text (.txt) file, and then click Open.
iv. Click **Import** button to import the list of IP addresses from the selected file.

Note:

- The text file should contain valid IP addresses with each entry in a separate line as shown below:



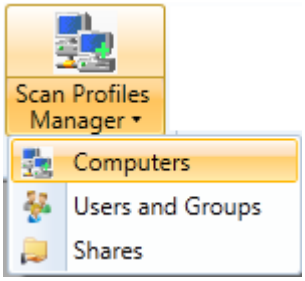
- During the import process each IP address will be translated to a corresponding computer name. Hence, only valid entries will be imported. To view the list of entries imported, click Verify Imported List button. The list of IP addresses and their corresponding computer names will be displayed as shown below:



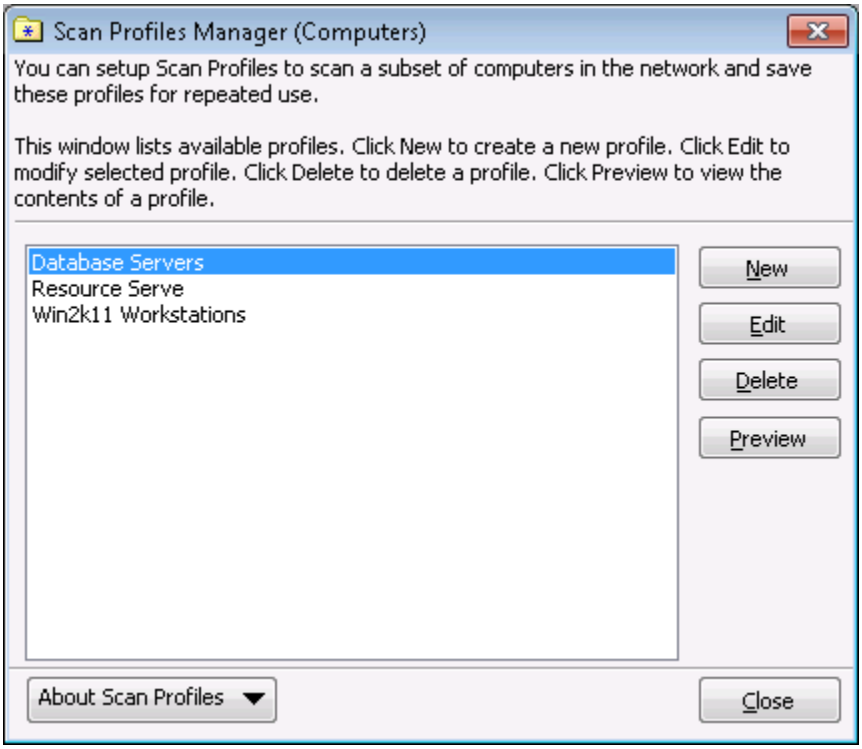
- Changes to the external text file will not automatically be reflected in the Scan Profile. You need to edit the Scan Profile and re-import the updated IP address list from the file.

4. Click **OK** to save the Scan Profile for later use.

How to manage Scan Profiles (Computers)?



Click in Configuration tab to launch the Scan Profiles Manager. The Scan Profiles Manager shows the list of Scan Profiles available.


Scan Profiles Manager (Computers)
You can setup Scan Profiles to scan a subset of computers in the network and save these profiles for repeated use.
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.
Database Servers
Resource Serve
Win2k11 Workstations
New
Edit
Delete
Preview
About Scan Profiles
Close

The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile
- Edit an existing Scan Profile
- Delete a Scan Profile
- Preview the list of computers in a Scan Profile

Create a new Scan Profile

1. To create a new Scan Profile click **New**
2. Follow the steps as outlined in How to create Scan Profiles?

Edit an existing Scan Profile

To edit a Scan Profile click **Edit** button in the Scan Profiles Manager. The Scan Profile Dialog will appear on the screen which will allow you to edit the selected Scan Profile.

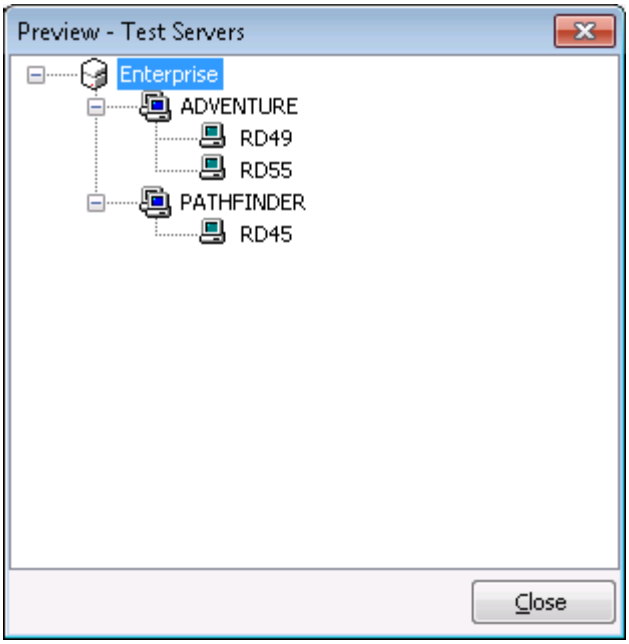
During edit operation you can modify the computer list, however, you cannot modify the type of the Scan Profile.

Delete a Scan Profile

To delete a Scan Profile, select the profile you want to delete, and then click **Delete** button. The selected Scan Profile will be deleted permanently. Please note, that reports associated with the Scan Profile deleted may fail to run when generated.

Preview the list of computers in a Scan Profile

To preview the list of computers in a Scan Profile, select a Scan Profile, and then click **Preview** button. The computer list will be displayed in a tree view as shown below:



The Preview window shows the list of domains and computers selected in the Scan Profile if the computer list was either imported or selected from the network. Whereas, if specific Windows versions were selected, then only the computers that match the selected Windows versions will show up. Furthermore, if specific domains were associated with the Scan Profile, then only the selected domains will show up, otherwise all the domains in the network will show up.

The Preview window allows you to view what computers in the network will be included in the profile.

How to apply Scan Profiles (Computers) in NTFS Security Auditor Module?

You can apply a Scan Profile to one or more reports to restrict the list of computers during report generation. This is especially useful if you want to generate reports for a subset of computers.

This page covers the following topics with regard to usage of Scan Profiles:

- Scan Profiles and Power Export Tool (off-line report generation)
- Scan Profiles and Interactive Report Generation

Scan Profiles and Power Export Tool (off-line report generation)

You can apply a Scan Profile to one or more reports using the Power Export Tool (for off-line generation) to restrict the domain scope and to scan and collect data for a subset of computers in the network. The report data will be collected for all computers in the applied Scan Profile. However, if the applied Scan Profile becomes unavailable during report generation (likely to happen if the Scan Profile is accidentally deleted), the report data will not be collected at all and will result in an error. Furthermore, if there are no computers to be found in the Scan Profile for a domain for which the report is being generated, then the report generation will fail as well. This is likely to happen if the domain is not included in the Scan Profile or none of the computers in the domain are running the Windows version setup in the Scan Profile.

Scan Profiles and Interactive Report Generation

You may also apply a Scan Profile to reports and view the data in interactive mode. The way in which a Scan Profile is applied and the data collection methodology adopted slightly differs in interactive mode from off-line report generation mode (using Power Export Tool). The data collection methodology adopted also depends on the type of Scan Profile applied (static or dynamic) to the report.

For instance, if a Scan Profile is associated with multiple domains, in interactive mode, data will be collected only for computers that belong to the currently selected domain. On the other hand, if there are no computers to be found for the currently selected domain, in the applied profile, the report data will not be collected at all. This is likely to happen if the currently selected domain was not included in Scan Profile (if it is a static profile) or the Scan Profile includes a Windows version filter, say Windows XP computers only, and the domain does not have any computers running Windows XP.

In addition, in interactive mode, there are differences on how Scan Profiles are applied to Domain-based Reports and Server-based Reports.

Scan Profiles and Domain-based Reports

In interactive mode, for domain-based reports, you can apply a Scan Profile by using the Scan Option Dialog. The report will be generated for the list of computers in the applied Scan Profile for the currently selected domain as mentioned earlier.

Scan Profiles and Server-based Reports

For server-based reports, you can apply a Scan Profile by clicking the button in the report window. The Scan Profiles Manager will show up on screen, select a Scan Profile, and then click Apply button to apply the selected profile.

For server-based reports, however, a Scan Profile when applied reloads the tree view, in the left pane in the report window, with the list of computers in the selected Scan Profile. After a Scan Profile is applied, you can select the desired computer in the tree view in the report window to generate the report. Click the Clear button to clear the applied profile. This will reload tree view with the list of all domains in the network.

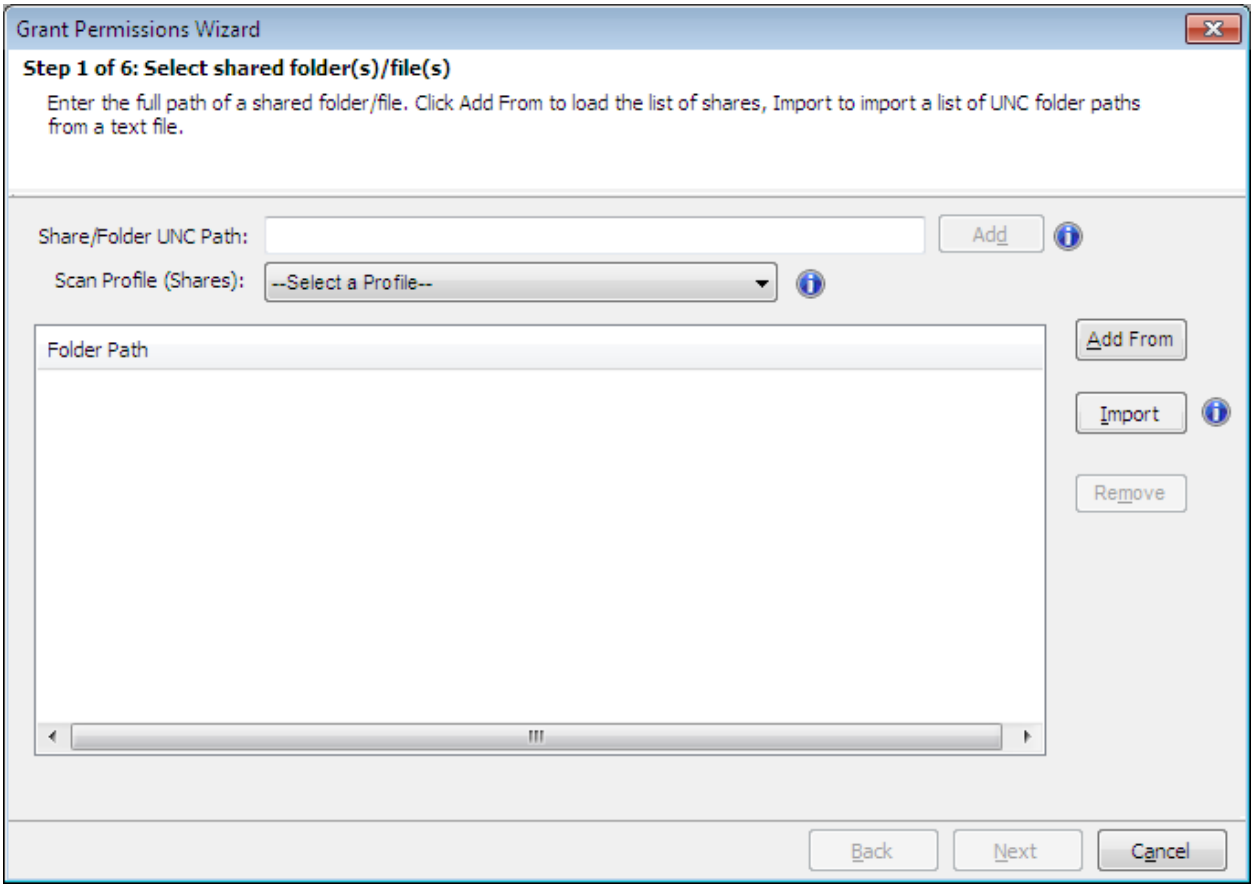
How to apply Scan Profiles (Computers) in NTFS Security Manager Module?

You can apply Scan Profile (Computers) to Grant Permissions, Revoke Permissions, Copy Permissions and also Modify Permissions that involves changes to permissions for the accounts on shared folder(s)/file(s). The following steps describe on how to apply Scan Profiles (computers) in the Grant Permissions wizard.

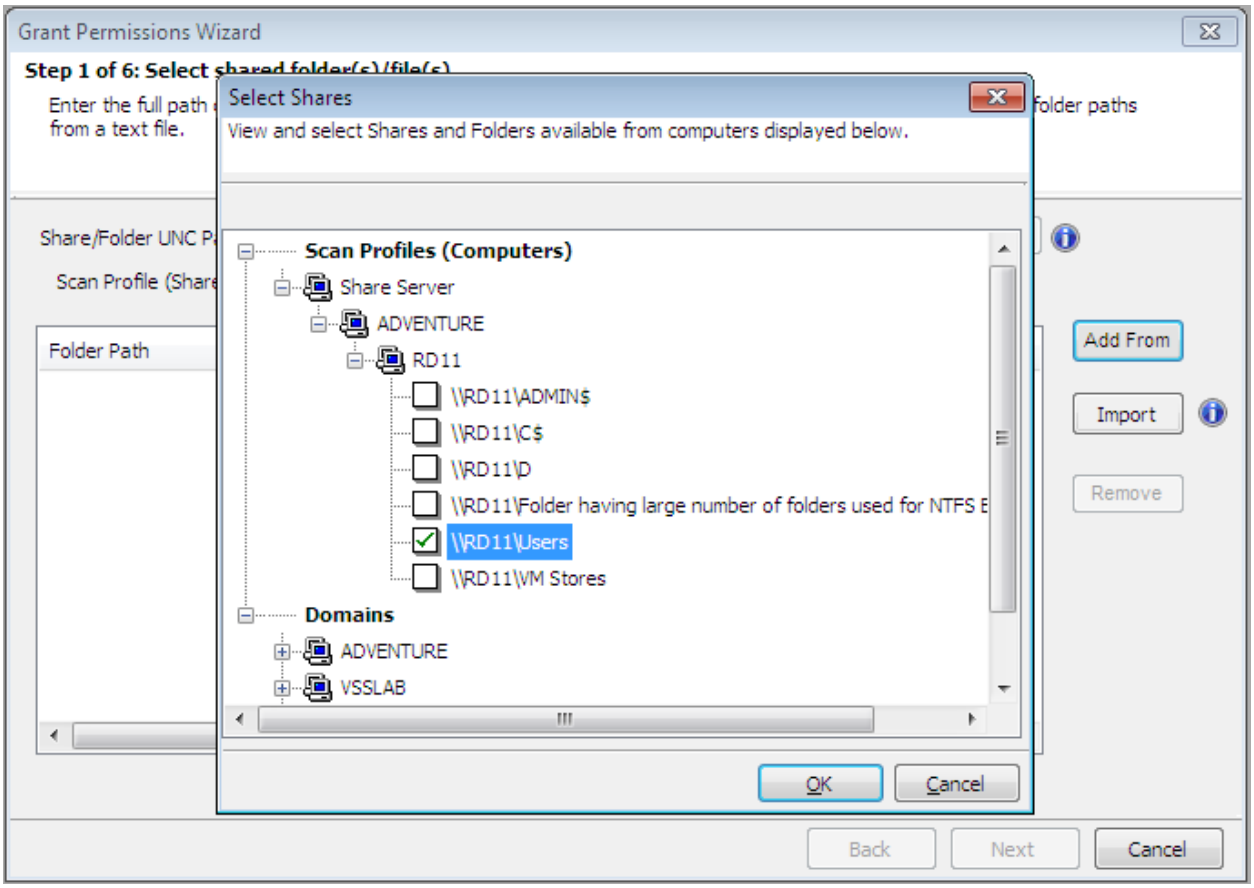
Click on

button in the toolbar.

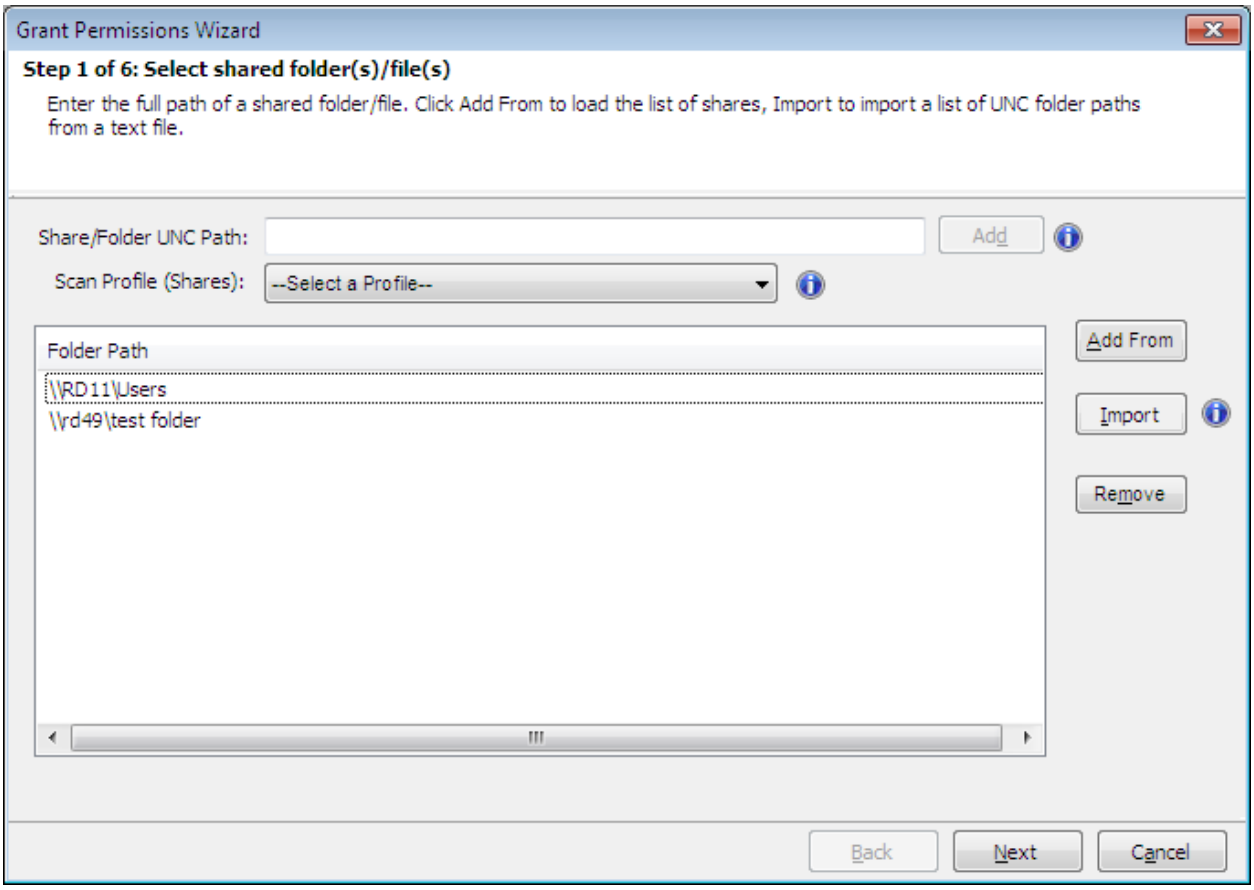
The Grant Permissions window will be displayed as shown below:


Grant Permissions Wizard
Step 1 of 6: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Back
Next
Cancel

- Click **Add From**
- Expand Select a Scan Profile (Computers) and enumerate servers in the profile to select its shared folder(s)/file(s)
- Select the shared folder(s)/file(s) displayed under the servers



- The selected shared folder(s)/file(s) will be added to the wizard as shown below:



- In the subsequent steps, select the necessary details for granting permissions for shared folder(s)/file(s) selected from Scan Profile (Computers) servers.

About Scan Profiles (Users/Groups)

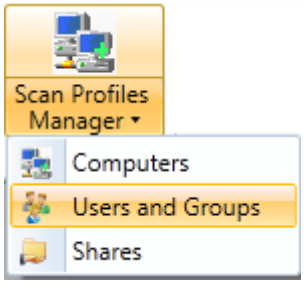
You can setup Scan Profiles (Users/Groups) to scan a subset of users/groups present in computers and save these profiles for repeated use (useful for repeatedly scanning and reporting on different subsets of users and groups permissions on share folders).

For more information about Scan Profiles (Users/Groups) follow the links given below.

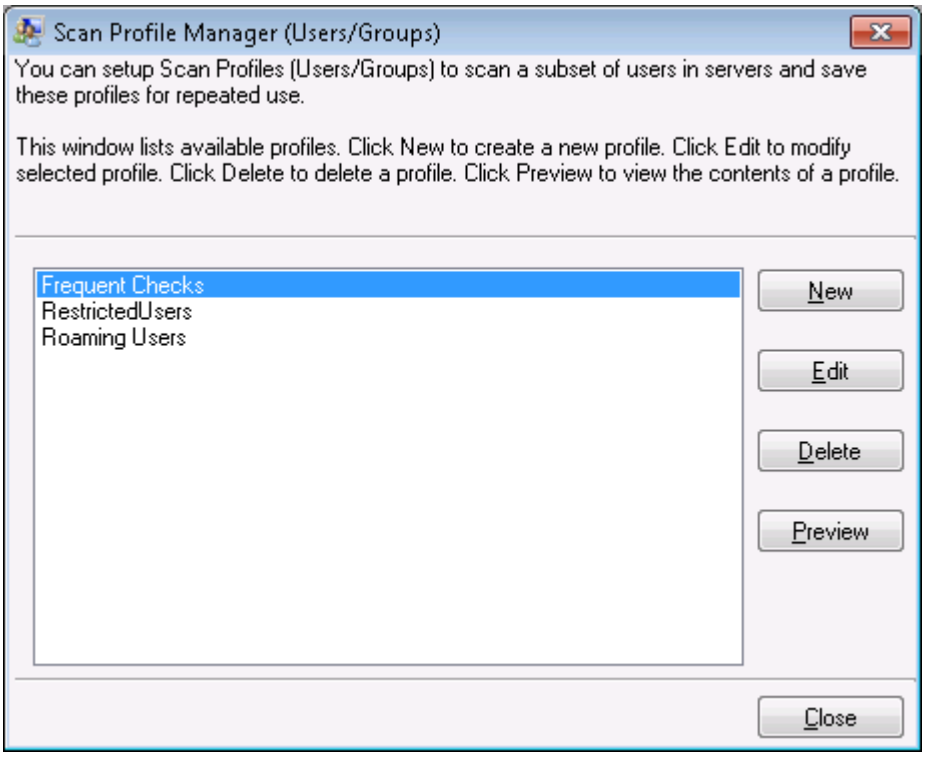
- How to create Scan Profiles (Users/Groups)?
- How to manage Scan Profiles (Users/Groups)?
- How to apply Scan Profiles (Users/Groups)?

How to create Scan Profiles (Users/Groups)?

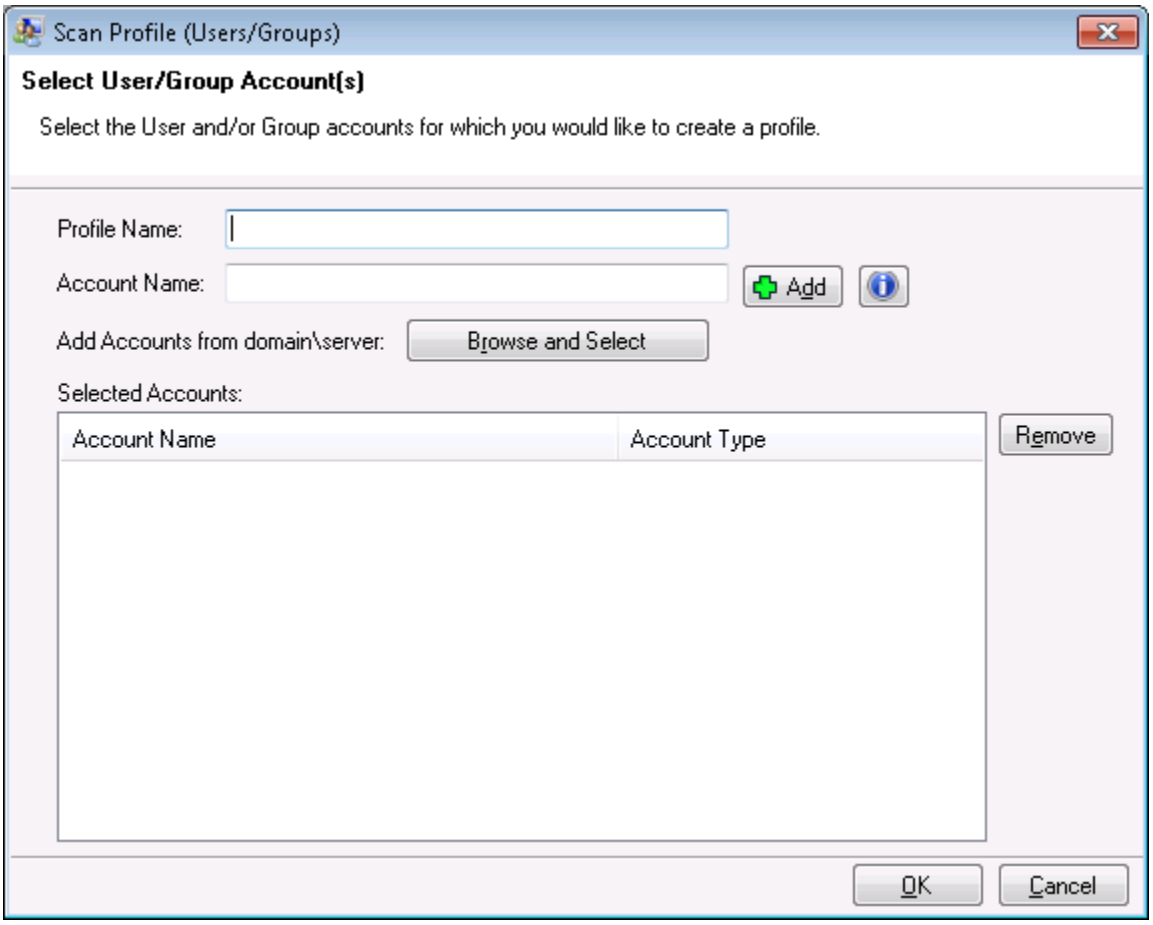
Perform the following steps to create a Scan Profile (Users/Groups).

1. Select 

from the Configuration tab. This action will launch the Scan Profiles Manager (Users/Groups) dialog as shown below.

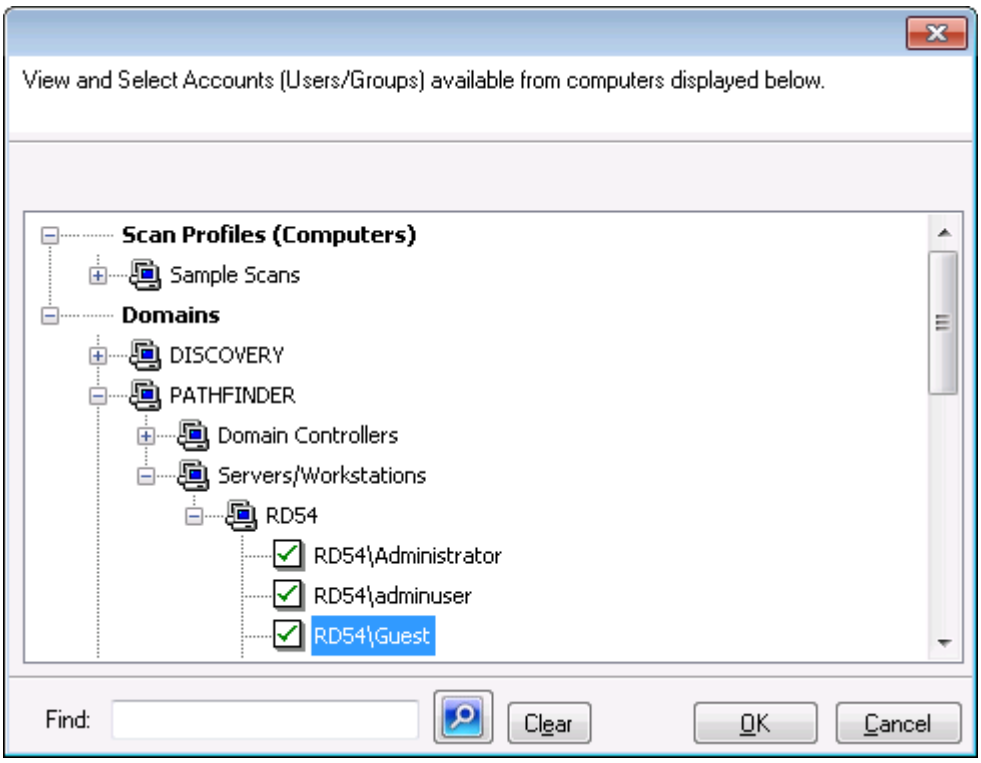

Scan Profile Manager (Users/Groups)
You can setup Scan Profiles (Users/Groups) to scan a subset of users in servers and save these profiles for repeated use.
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.
Frequent Checks
RestrictedUsers
Roaming Users
New
Edit
Delete
Preview
Close

2. Click **New** button in the Scan Profiles Manager (Users/Groups) dialog. This action will launch the Scan Profiles (Users/Groups) dialog as shown below.

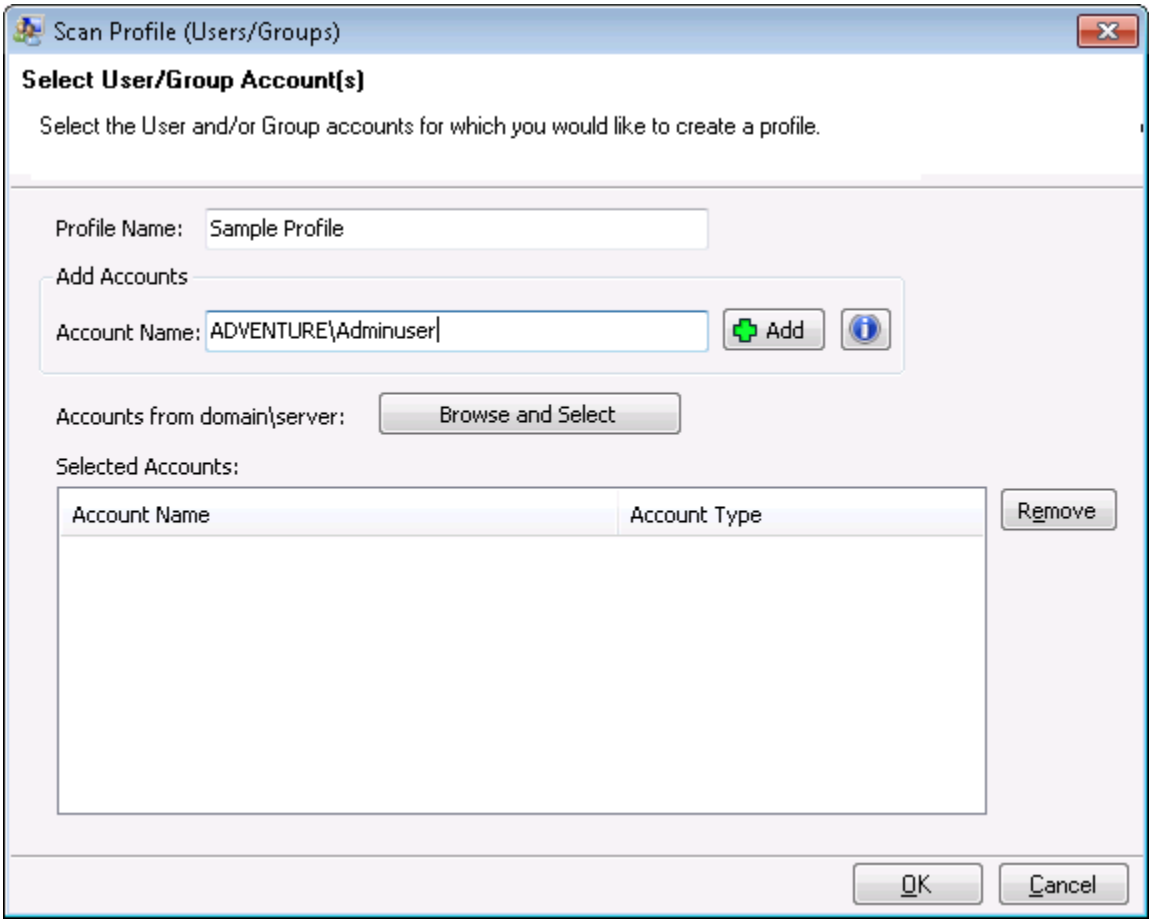


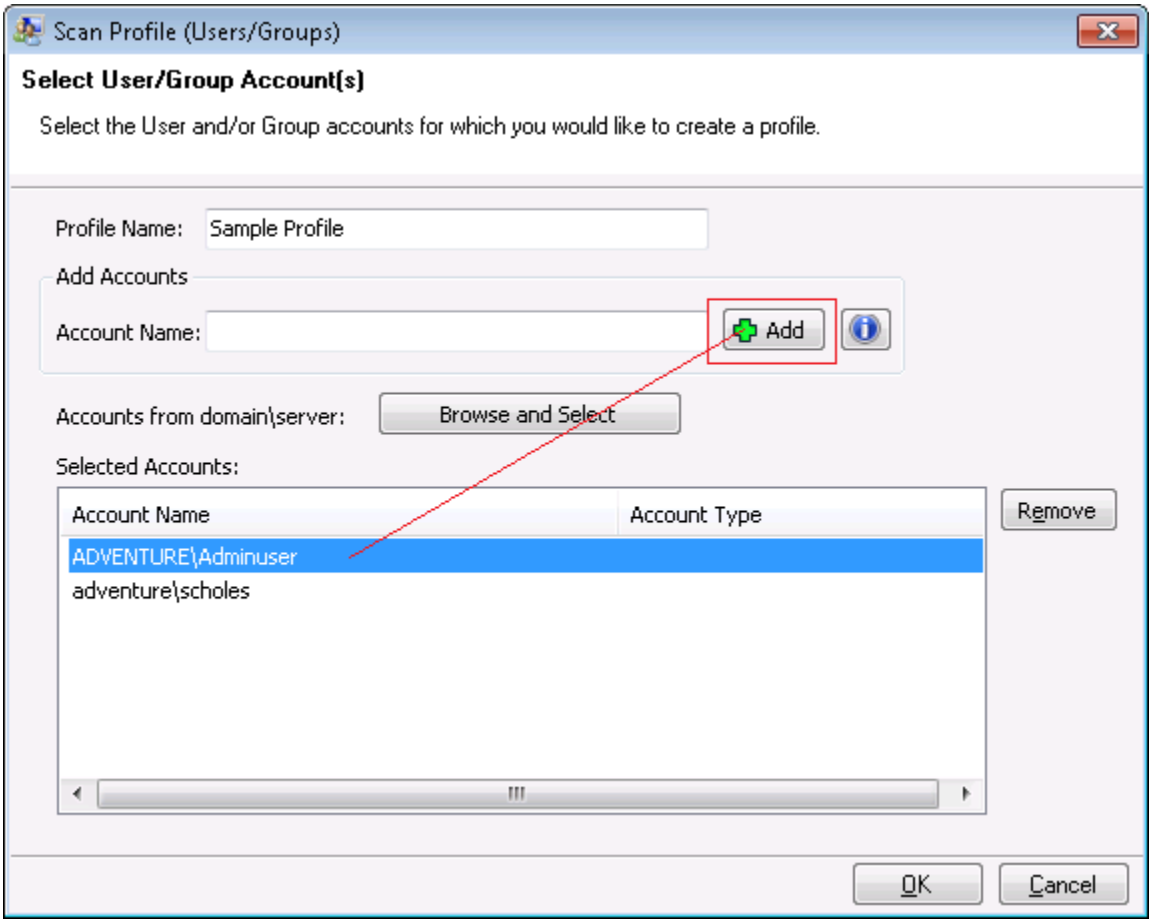
1. Enter a name for the profile.

2. Use the Browse and Select button to enumerate users/groups from servers or Scan Profiles Computers as shown below



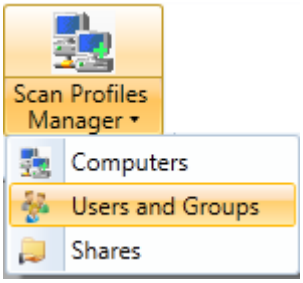
3. You can enter users / groups name and add to the selected account list for creating a profile. Enter the users/groups name in 'Domain\User Name' format and click the Add button to add the entered account to the list as shown below.


Scan Profile (Users/Groups)
Select User/Group Account(s)
Select the User and/or Group accounts for which you would like to create a profile.
Profile Name:
Sample Profile
Add Accounts
Account Name:
ADVENTURE\Adminuser
Add
Accounts from domain\server:
Browse and Select
Selected Accounts:
Account Name
Account Type
Remove
OK
Cancel

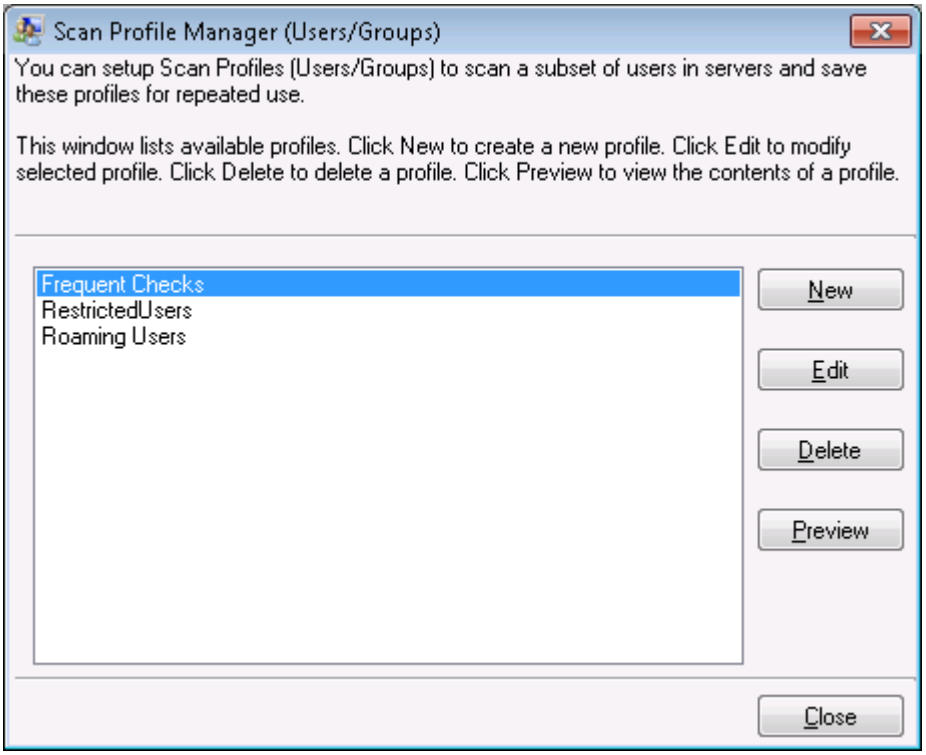


5. Click Finish to save the Users/Groups profile for future use.

How to manage Scan Profiles (Users/Groups)?



Click to launch the Scan Profiles Manager (Users/Groups). The Scan Profiles Manager (Users/Groups) shows the list of available profiles.


Scan Profile Manager (Users/Groups)
You can setup Scan Profiles (Users/Groups) to scan a subset of users in servers and save these profiles for repeated use.
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.
Frequent Checks
RestrictedUsers
Roaming Users
New
Edit
Delete
Preview
Close

The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile (Users/Groups)
- Edit an existing Scan Profile (Users/Groups)
- Delete a Scan Profile (Users/Groups)
- Preview the list of users and groups in a Scan Profile (Users/Groups)

Create a new Scan Profile (Users/Groups)

1. To create a new Scan Profile (Users/Groups) click New
2. Follow the steps as outlined in How to create Scan Profiles?

Edit an existing Scan Profile (Users/Groups)

To edit a Scan Profile (Users/Groups) click Edit button in the Scan Profiles Manager. The Scan Profile (Users/Group) wizard will appear on the screen which will allow you to edit the selected profile.

During edit operation you can modify the Users/Groups list.

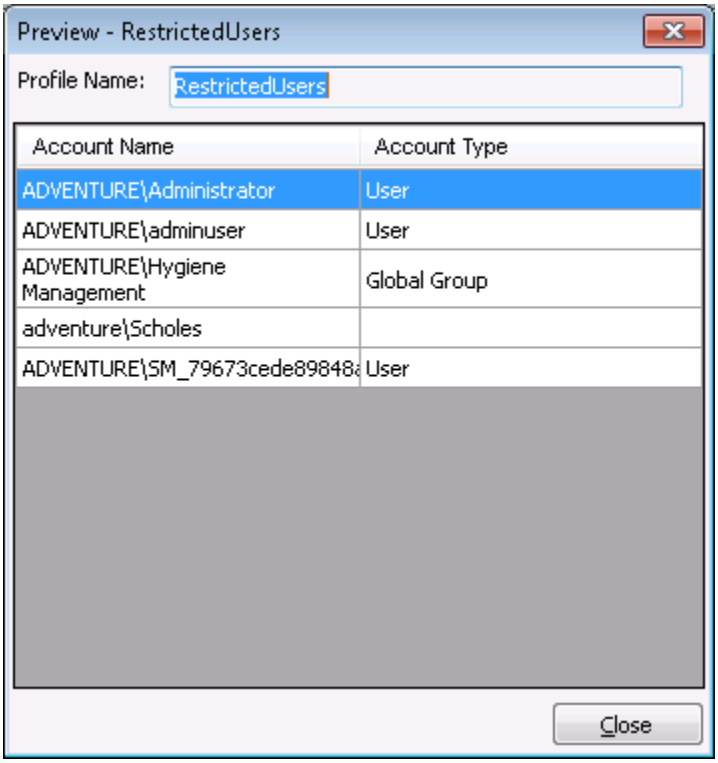
Delete a Scan Profile (Users/Groups)

To delete a Scan Profile (Users/Groups), select the profile you want to delete, and then click Delete button. The selected Scan Profile (Users/Groups) will be deleted permanently.

Please note, that reports associated with the Scan Profile (Users/Groups) deleted may fail to run when generated.

Preview the list of users and groups in a Scan Profile (Users/Groups)

To preview the list of users and groups in a profile, select a profile, and then click Preview button.



The Preview window allows you to view what users and groups will be included in the profile.

How to apply Scan Profiles (Users/Groups) in NTFS Security Auditor Module?

You can apply Scan Profile (Users/Groups) to permissions reports that involves generating permissions for specific users and groups on share folders. This is especially useful, if you want to generate permissions reports for certain users and groups frequently.

The following shows permissions reports that involves specific users and groups.

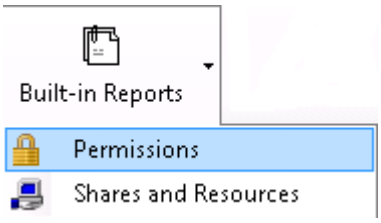
Report Name	Description
List of permissions for specific users and groups on folders	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
List of permissions for specific users and groups on files	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.
List of effective permissions for specific users and groups on folders	Reports the effective permissions for specific users and groups available in a set of folders.
List of effective permissions for specific users and groups on files	Reports the effective permissions for specific users and groups for files available in a set of folders.

Scan Profiles (Users and Groups) and permission reports for specific users and groups

You can apply a Scan Profile (Users/Groups) to permissions reports either using Power Export Tool (for off-line generation) or Interactive Report Generation .This option will useful, if permissions for certain Users and Groups need to be monitored frequently. Rather than searching for Users and Groups, adding then to account list and viewing their permissions. You can use the - create a subset of Users and Groups, save them as a profile, generating permissions reports for subset that of users and groups. The following shows how Scan Profiles (Users/Groups) can be applied to permission reports for specific users and groups in Interactive report generation and Power export tool.

Scan Profiles (Users/Groups) and Interactive Report Generation

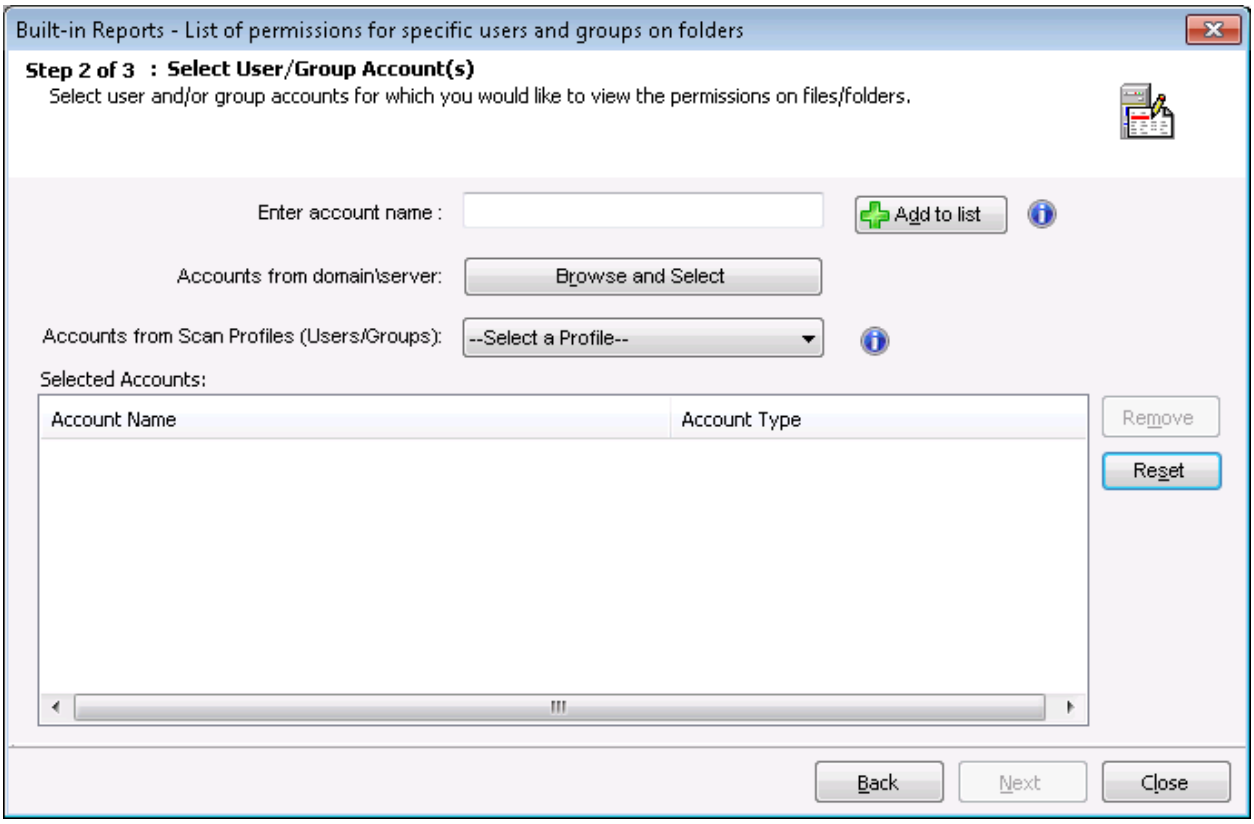
Perform the following steps for applying Scan Profiles (Users/Groups) to permission reports in Interactive report generation

Click on 

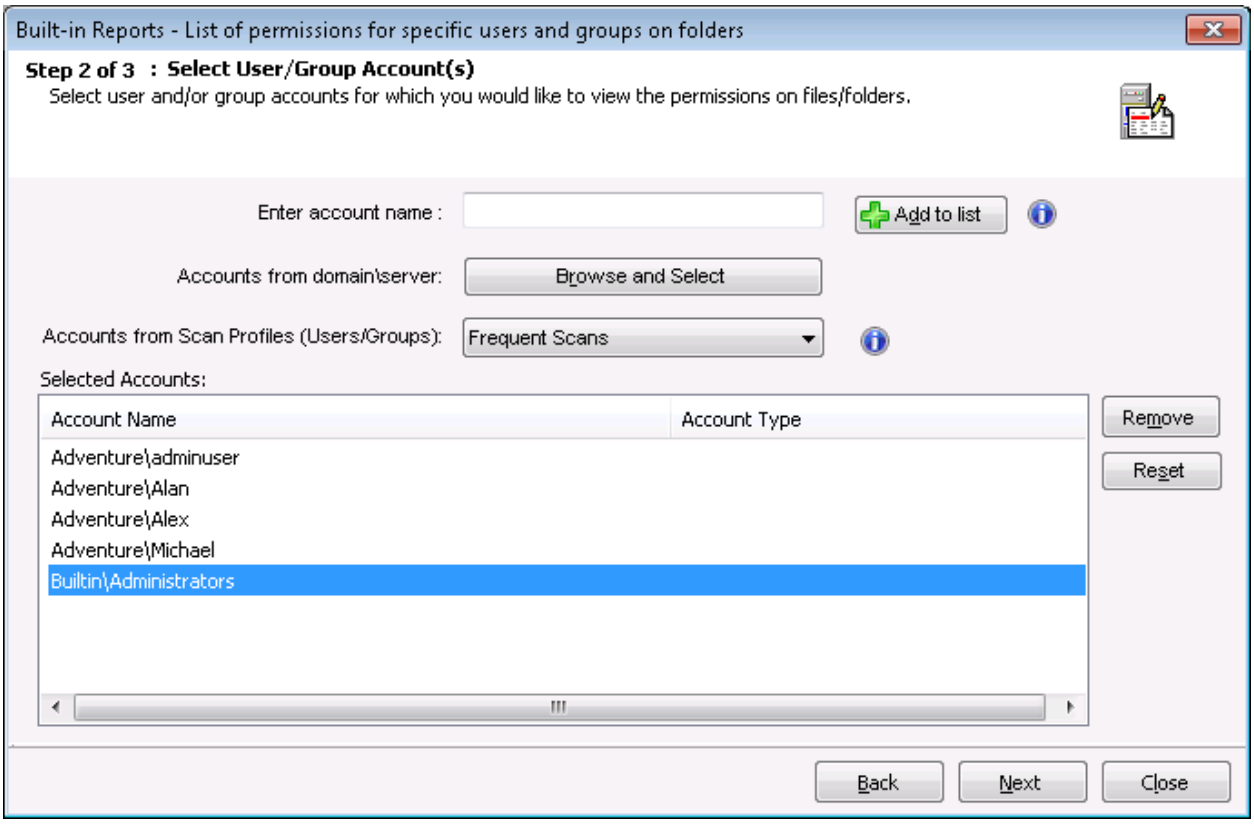
under Built-in Reports in the tool bar.

- Select any one of the permissions reports listed above and click Next to proceed.

- In the next step, select the option 'Select a Scan Profiles (Users/Groups) ' as shown below.


Built-in Reports - List of permissions for specific users and groups on folders
Step 2 of 3 : Select User/Group Account(s)
Select user and/or group accounts for which you would like to view the permissions on files/folders.
Enter account name :
Add to list
Accounts from domain\server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
--Select a Profile--
Selected Accounts:
Account Name
Account Type
Remove
Reset
Back
Next
Close

- In this step the list of users and / or groups present in Scan Profile (Users/Groups) will be loaded to the selected account list as shown below.



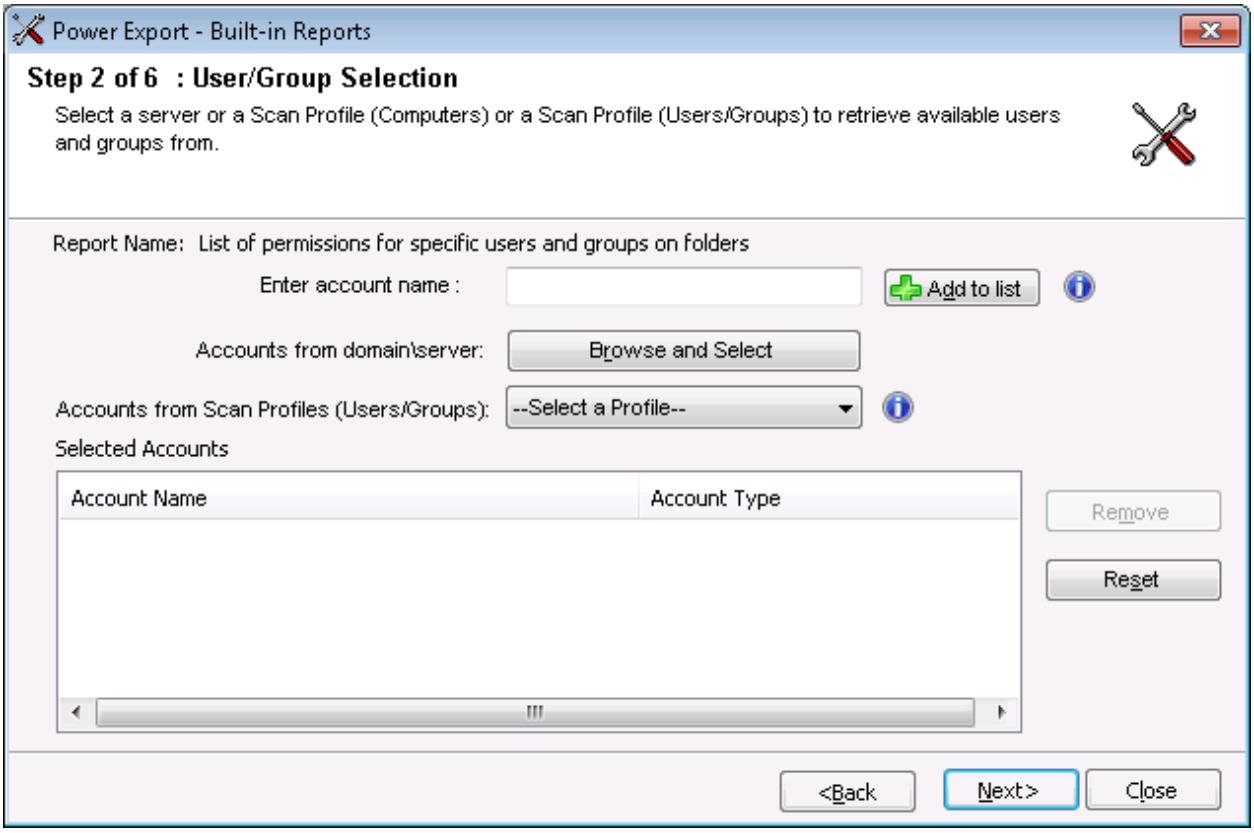
- In the succeeding steps select needed details for generating reports for selected users and groups.

Scan Profiles (Users/Groups) and Power Export Tool (off-line report generation)

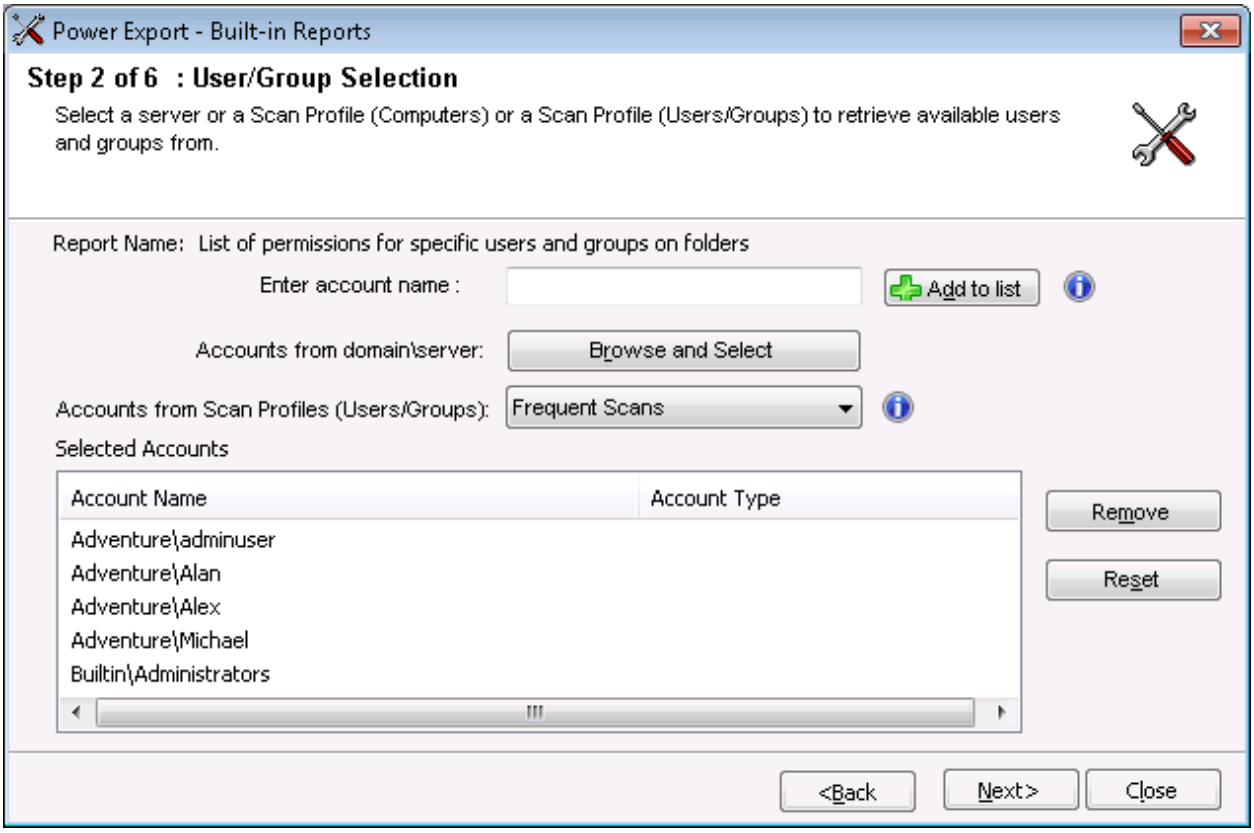
You can apply a Scan Profile (Users/Groups) to permissions reports using Power Export Tool (for off-line generation).

- Click on button in the toolbar.

- Select any one of the permissions reports listed above and click Next to proceed.
- In the next step, select the option 'Select a Scan Profiles (Users/Groups)' as shown below.


Power Export - Built-in Reports
Step 2 of 6 : User/Group Selection
Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.
Report Name: List of permissions for specific users and groups on folders
Enter account name :
Add to list
Accounts from domain\server:
Browse and Select
Accounts from Scan Profiles (Users/Groups):
--Select a Profile--
Selected Accounts
Account Name
Account Type
Remove
Reset
<Back
Next>
Close

- In this step the list of users and groups present in Scan Profile (Users/Groups) will be loaded to the selected account list as shown below.



- In the succeeding steps select needed details for generating reports for selected Scan Profile (Users/Groups).

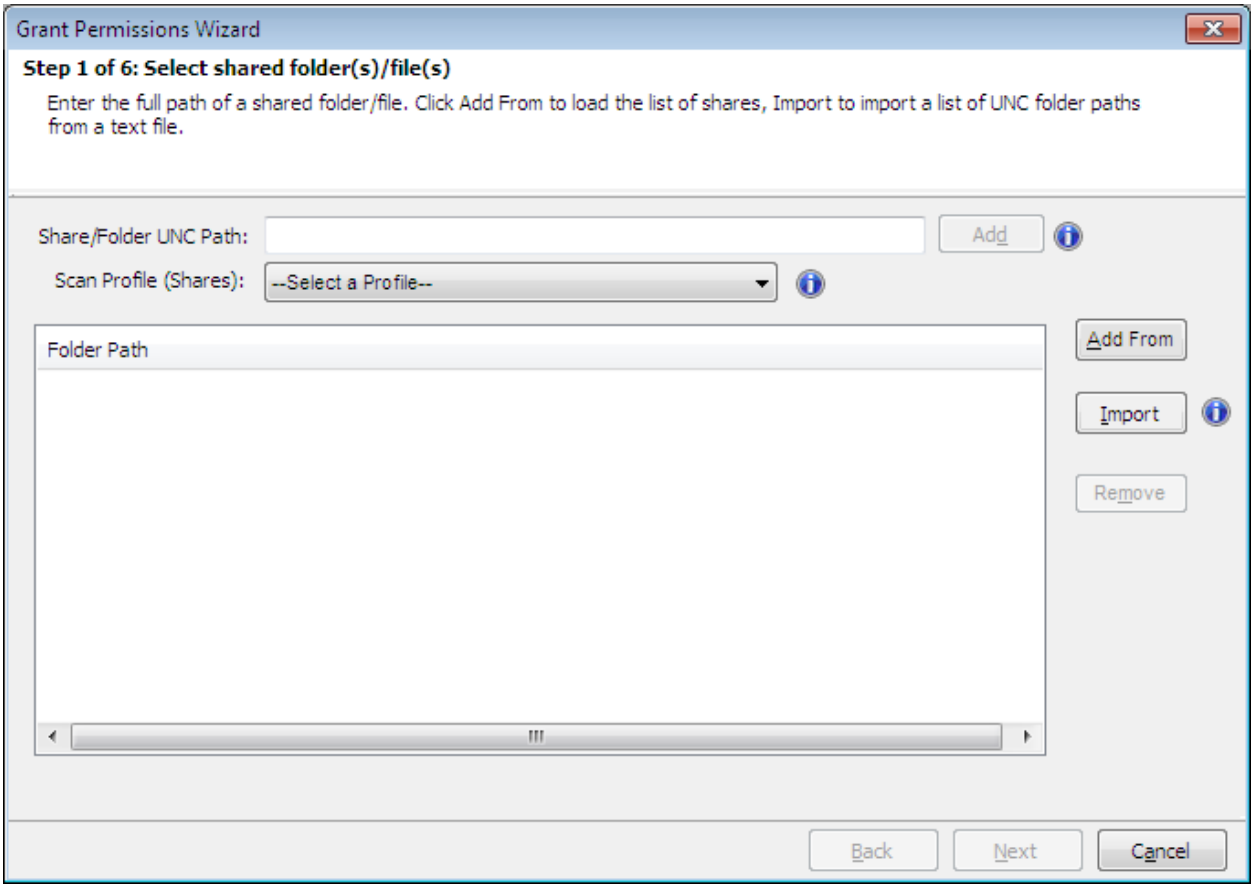
How to apply Scan Profiles (Users/Groups) in NTFS Security Manager Module?

You can apply Scan Profile (Users/Groups) to Grant Permissions, Revoke Permissions and also Modify Permissions that involves changes to permissions for the accounts on shared folder(s)/file(s). The following steps describe on how to apply Scan Profiles (User/Groups) in the Grant Permissions wizard.

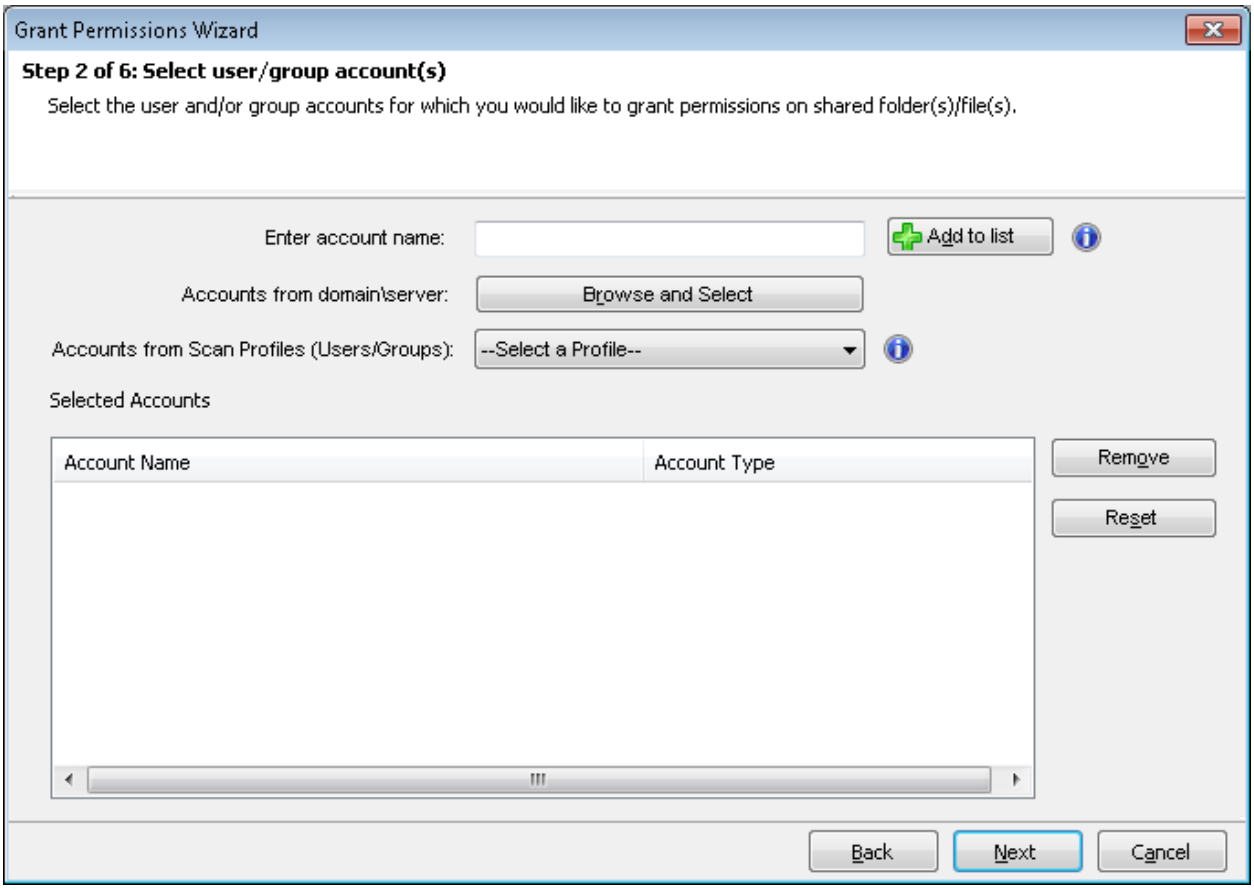
Click on

button in the toolbar.

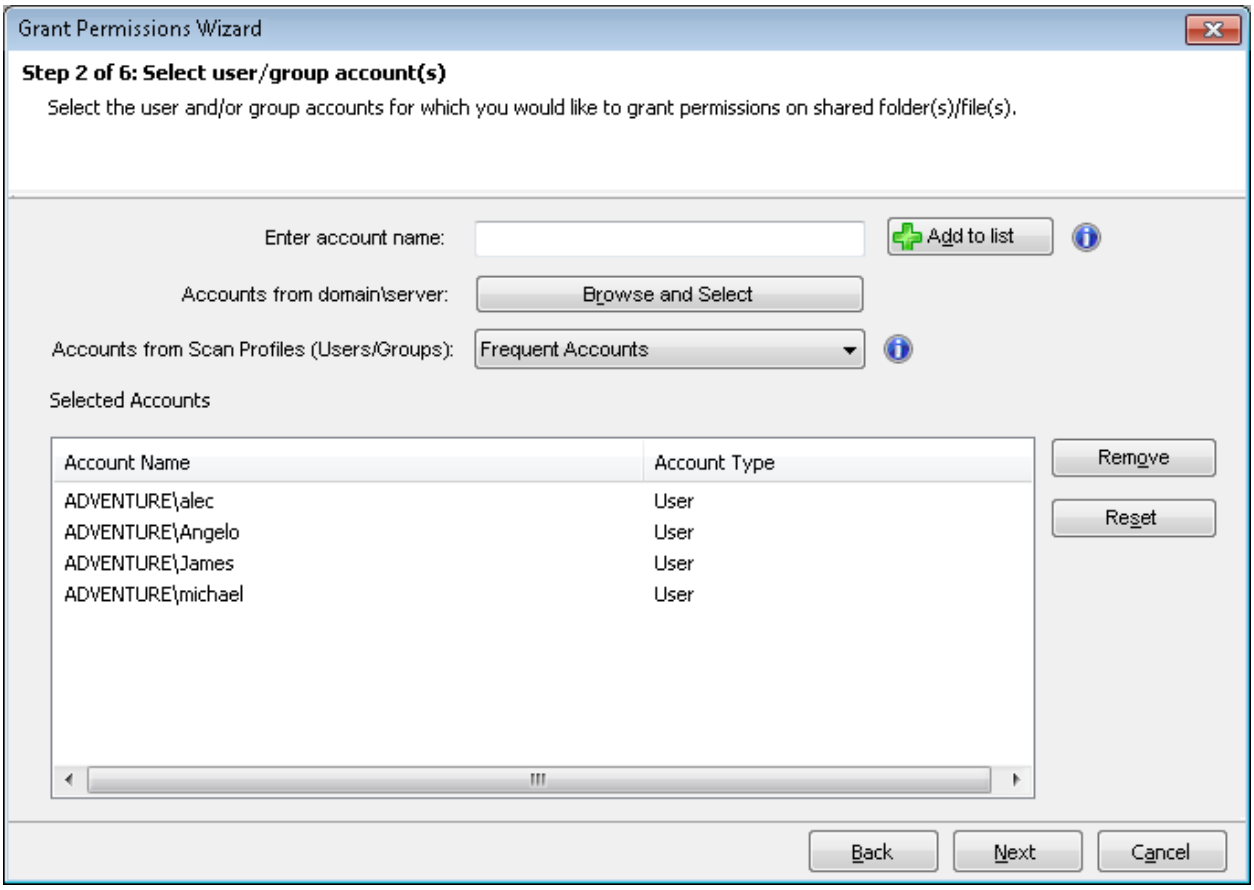
The Grant Permissions window will be displayed as shown below:


Grant Permissions Wizard
Step 1 of 6: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Back
Next
Cancel

- Select one or more shared folder(s)/files(s) and click Next to proceed.
- In Select user/group accounts step, select a profile from the Scan Profile (Users/Groups) dropdown to use the users/groups added in a profile.



- The list of users and groups present in the selected Scan Profile (Users/Groups) will be loaded to the wizard as shown below.



- In the subsequent steps, select the necessary details for granting permissions for accounts present in the Scan Profile (Users/Groups).

About Scan Profiles (Shares)

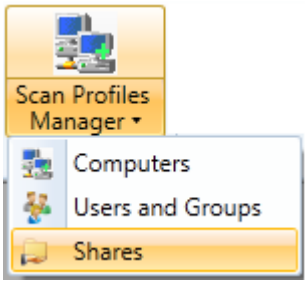
You can setup Scan Profiles (Shares) to scan a subset of shares present in computers and save these profiles for repeated use (useful for repeatedly scanning and reporting on different subsets of share folders permissions).

For more information about Scan Profiles (Shares) follow the links given below.

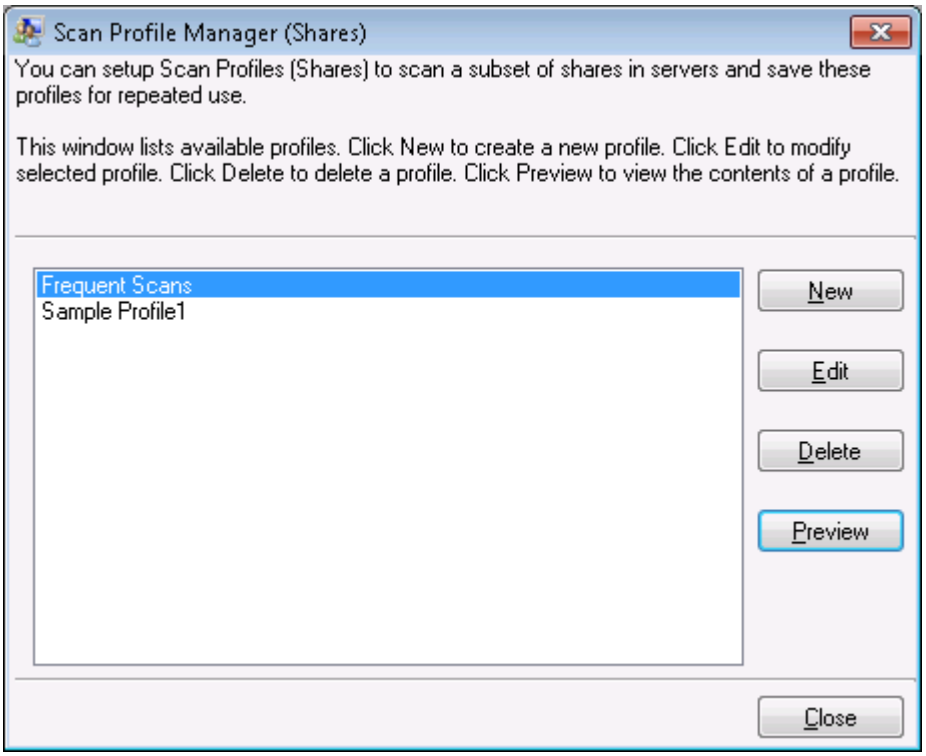
- How to create Scan Profiles (Shares)?
- How to manage Scan Profiles (Shares)?
- How to apply Scan Profiles (Shares)?

How to create Scan Profiles (Shares)?

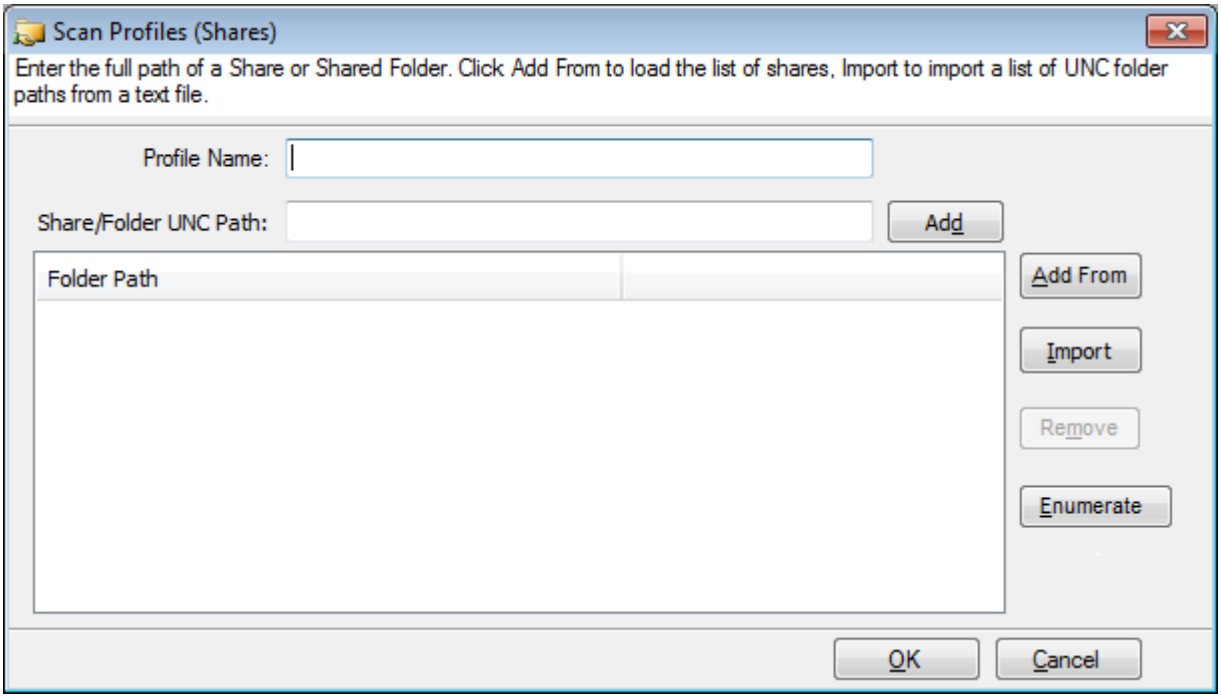
Perform the following steps to create a Scan Profiles (Shares).

1. Select 

from the Configuration tab. This action will launch the Scan Profiles Manager (Shares) dialog as shown below.

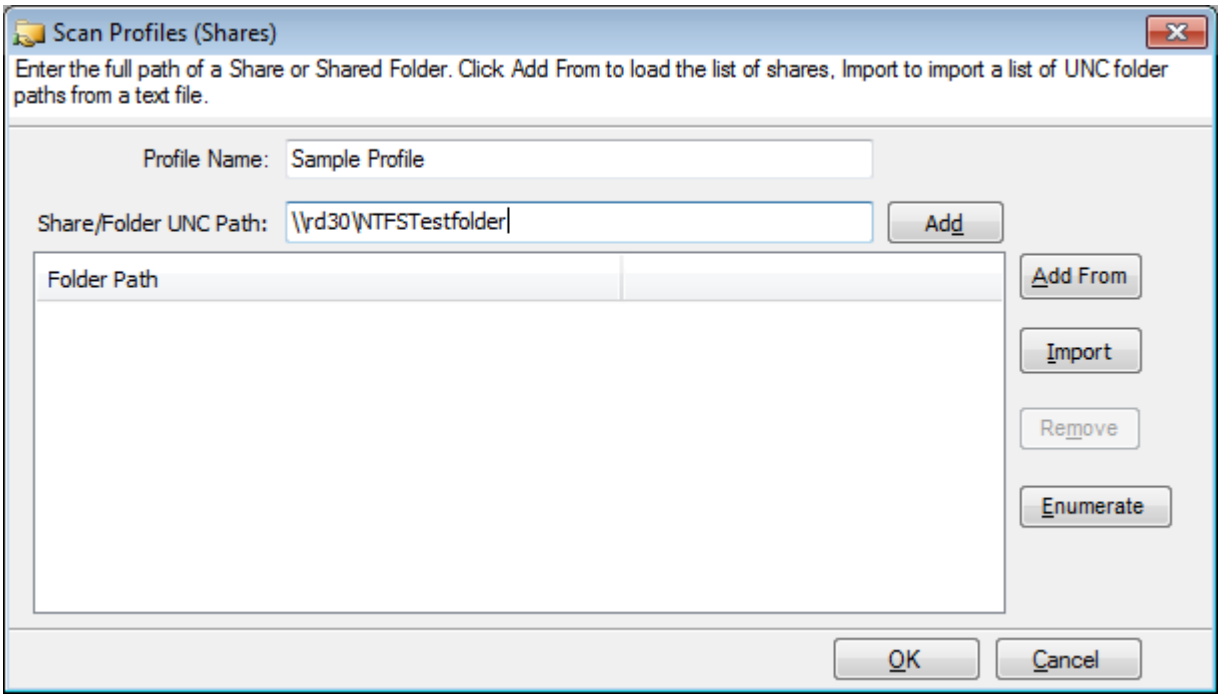

Scan Profile Manager (Shares)
You can setup Scan Profiles (Shares) to scan a subset of shares in servers and save these profiles for repeated use.
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.
Frequent Scans
Sample Profile1
New
Edit
Delete
Preview
Close

2. Click **New** button in the Scan Profiles Manager (Shares) dialog. This action will launch the Scan Profiles (Shares) dialog as shown below.


Scan Profiles (Shares)
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Profile Name:
Share/Folder UNC Path:
Add
Folder Path
Add From
Import
Remove
Enumerate
OK
Cancel

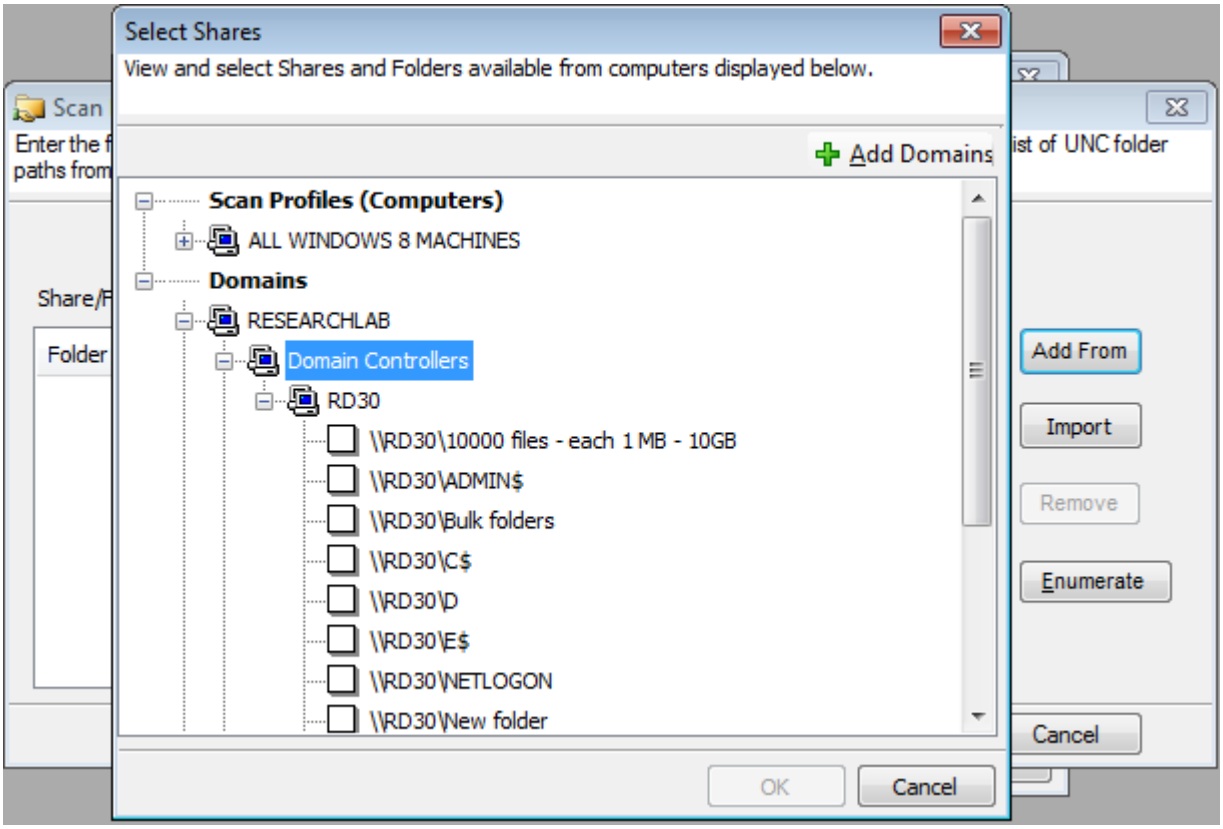
1. Enter a name for the profile.

2. You may type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list as shown below.

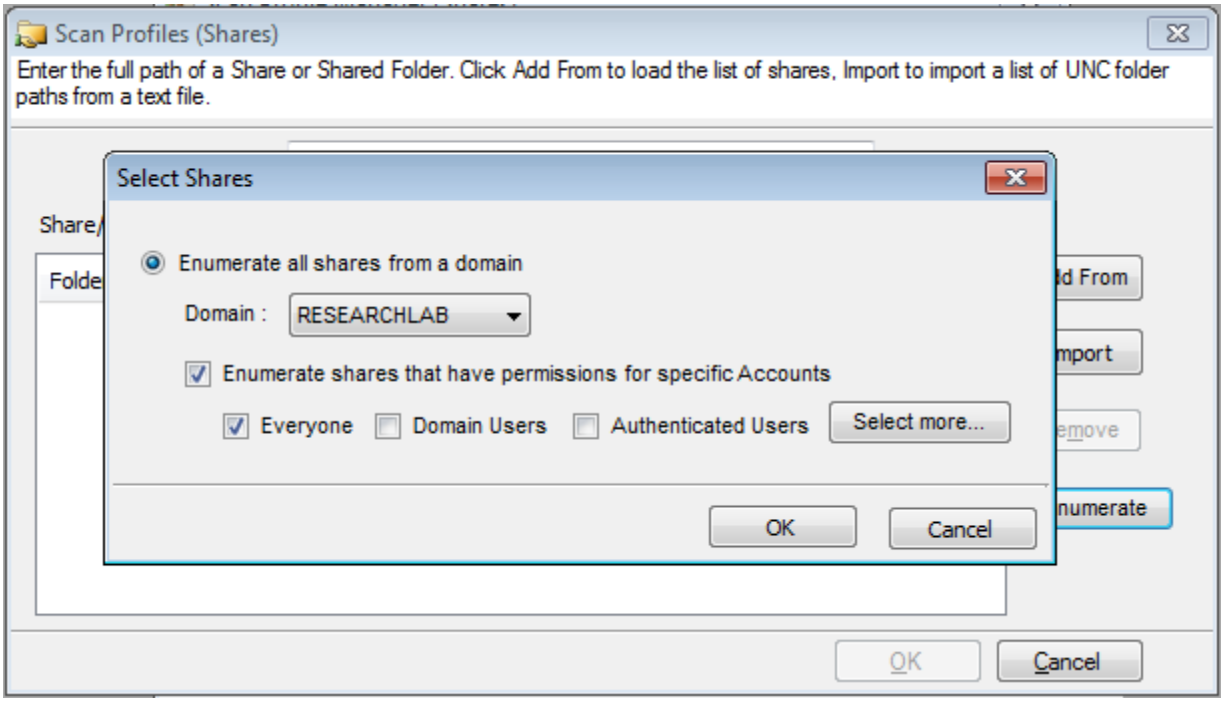


3. You may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

4. Click 'Add From' to add list of shared folders from computers as shown below.

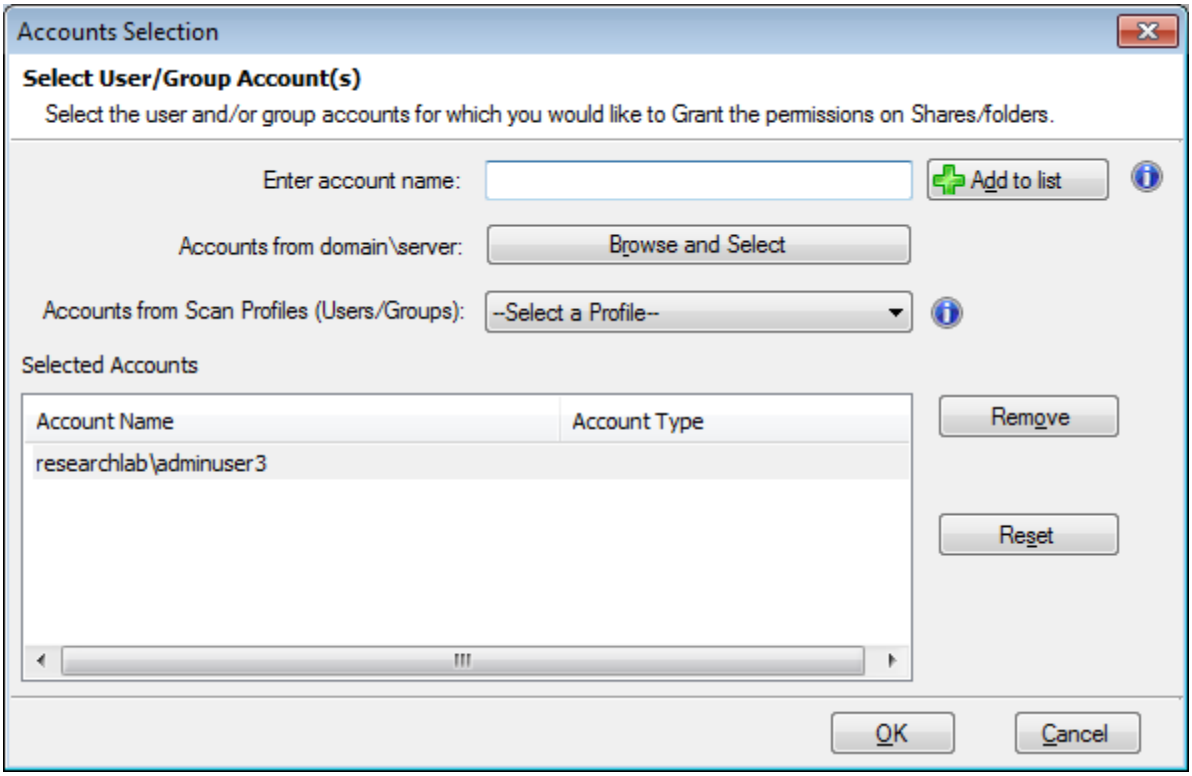


5. You can use 'Enumerate' option to scan the entire domain and find all file shares for which the selected accounts have permissions. Click **Enumerate** option. The 'Select Shares' dialog will be displayed as shown below.

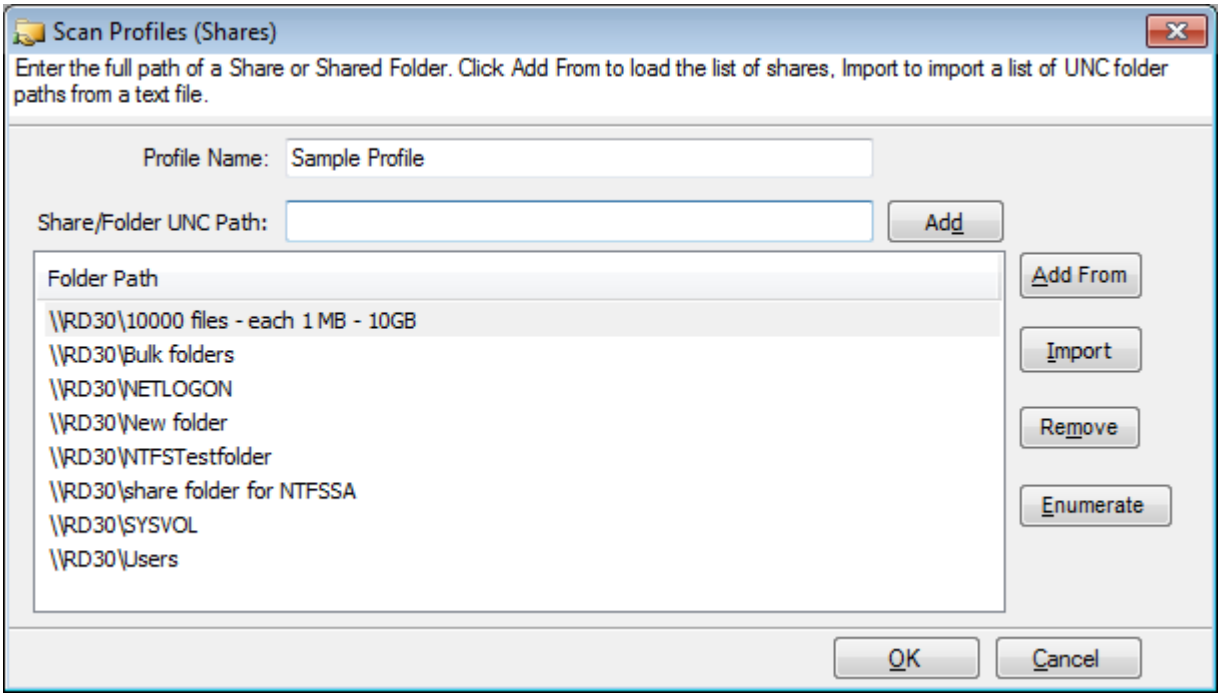


Select a domain and the desired accounts (say, Everyone) in order to filter the list of shares for which the specified user account (Everyone) has permissions defined.

Select a domain and the desired accounts (say, Everyone) in order to filter the list of shares for which the specified user account (Everyone) has access. If you want to scan with more accounts, click 'Select more...' and then select the accounts in 'Account Selection' dialog. Once accounts selection is complete, click 'OK' in 'Account Selection' dialog.

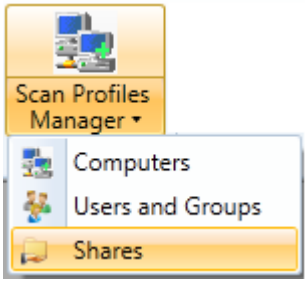


Click 'OK' in 'Select Shares'.

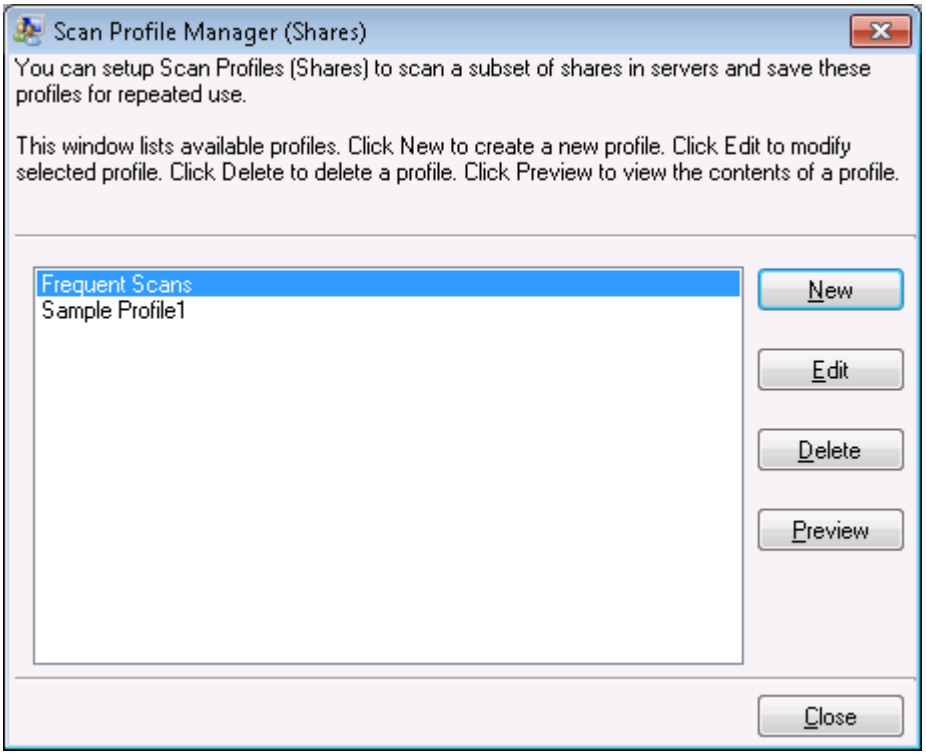


5. Click OK to save the Shares profile for future use.

How to manage Scan Profiles (Shares)?



Click to launch the Scan Profiles Manager (Shares). The Scan Profiles Manager (Shares) shows the list of available profiles.


Scan Profile Manager (Shares)
You can setup Scan Profiles (Shares) to scan a subset of shares in servers and save these profiles for repeated use.
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.
Frequent Scans
Sample Profile1
New
Edit
Delete
Preview
Close

The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile (Shares)
- Edit an existing Scan Profile (Shares)
- Delete a Scan Profile (Shares)
- Preview the list of Shares in a Scan Profile (Shares)

Create a new Scan Profile (Shares)

1. To create a new Scan Profile (Shares) click **New**
2. Follow the steps as outlined in How to create Scan Profiles?

Edit an existing Scan Profile (Shares)

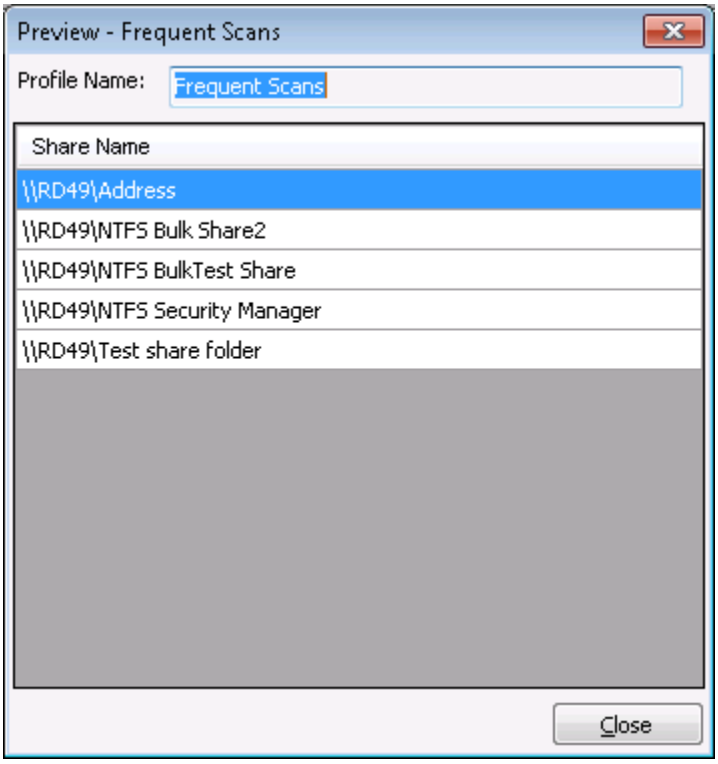
1. To edit a Scan Profile (Shares) click **Edit** button in the Scan Profiles Manager. The Scan Profile (Shares) wizard will appear on the screen which will allow you to edit the selected profile.
2. During edit operation you can modify the Shares list.

Delete a Scan Profile (Shares)

To delete a Scan Profile (Shares), select the profile you want to delete, and then click **Delete** button. The selected Scan Profile (Shares) will be deleted permanently. Please note, that reports associated with the Scan Profile (Shares) deleted may fail to run when generated.

Preview the list of shares in a Scan Profile (Shares)

To preview the list of shares in a profile, select a profile, and then click **Preview** button.



The Preview window allows you to view what shares will be included in the profile.

How to apply Scan Profiles (Shares) in NTFS Security Auditor Module?

You can apply Scan Profile (Shares) to permissions reports. This is especially useful, if you want to generate permissions reports for certain Shares frequently.

The following shows permissions reports that involves shares profile

List of Permissions Reports:

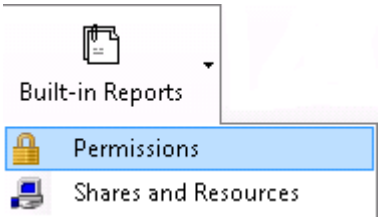
Report Name	Description
List of permissions for specific users and groups on folders	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
List of permissions for folders	Reports the permissions associated with a selected set of folders.
List of permissions for specific users and groups on files	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.
List of permissions for files	Reports the permissions associated with files under a selected set of folders.
List of all permissions for folders (Inherit & Explicit)	Reports the permissions for users assigned in the folders directly and inherited by means of nested groups.
List of effective permissions for users and groups on folders	Reports the effective permissions for users and groups for a set of folders.
List of effective permissions for users and groups on files	Reports the effective permissions for users and groups for files available in a set of folders.
List of effective permissions for specific users and groups on folders	Reports the effective permissions for specific users and groups available in a set of folders.
List of effective permissions for specific users and groups on files	Reports the effective permissions for specific users and groups for files available in a set of folders.

Scan Profiles (Shares) and permission reports

You can apply a Scan Profile (Shares) to permissions reports either using Power Export Tool (for off-line generation) or Interactive Report Generation .This option will useful, if permissions for certain shares need to be monitored frequently. Rather than searching for shares, adding them to list and viewing their permissions. You can create a subset of shares, save them as a profile, generating permissions reports for them. The following shows how Scan Profiles (Shares) can be applied to permission reports in Interactive report generation and Power export tool.

Scan Profiles (Users/Groups) and Interactive Report Generation

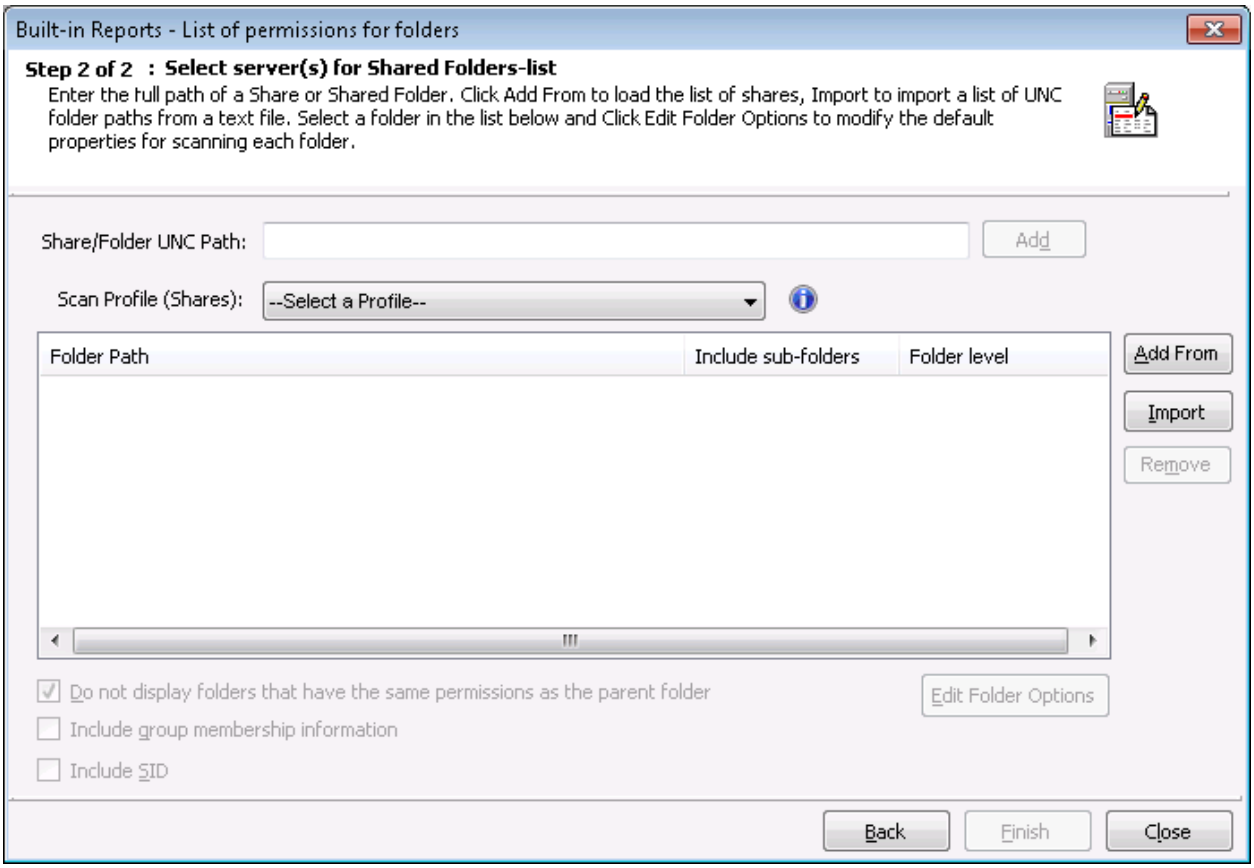
Perform the following steps for applying Scan Profiles (Shares) to permission reports in Interactive report generation

Click on 

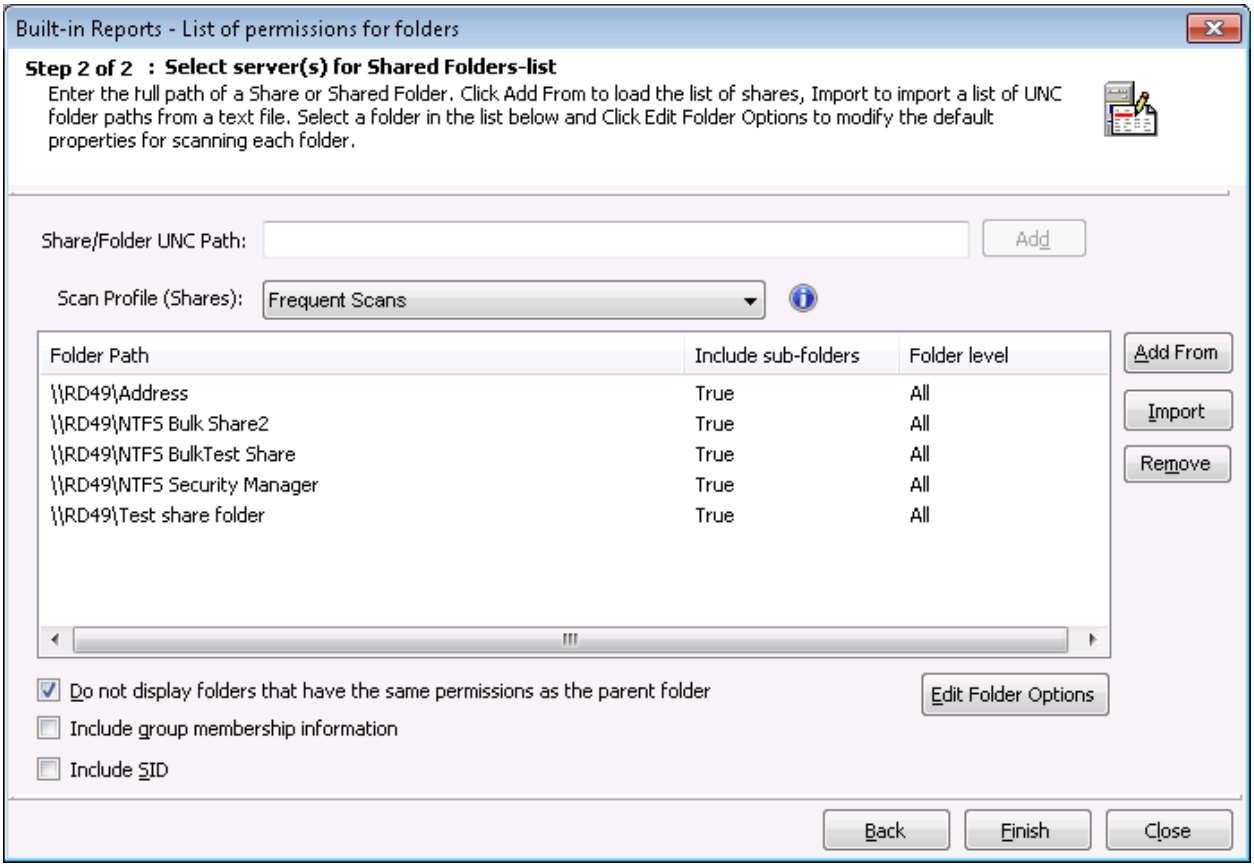
under Built-in Reports in the tool bar.

Select any one of the permissions reports listed above and click Next to proceed.

In the next step, select the option 'Select a Scan Profiles (Shares) ' as shown below.


Built-in Reports - List of permissions for folders
Step 2 of 2 : Select server(s) for Shared Folders-list
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-folders
Folder level
Add From
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options
Include group membership information
Include SID
Back
Finish
Close

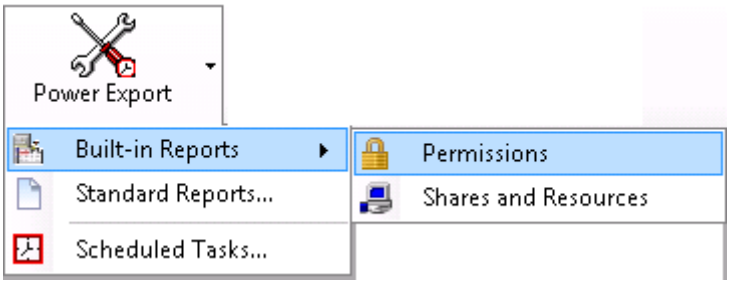
- In this step the list of shares present in Scan Profile (Shares) will be loaded to the selected account list as shown below.



- In the succeeding steps select needed details for generating reports for selected shares.

Scan Profiles (Users/Groups) and Power Export Tool (off-line report generation)

You can apply a Scan Profiles (Shares) to permissions reports using Power Export Tool (for off-line generation).

Click on 

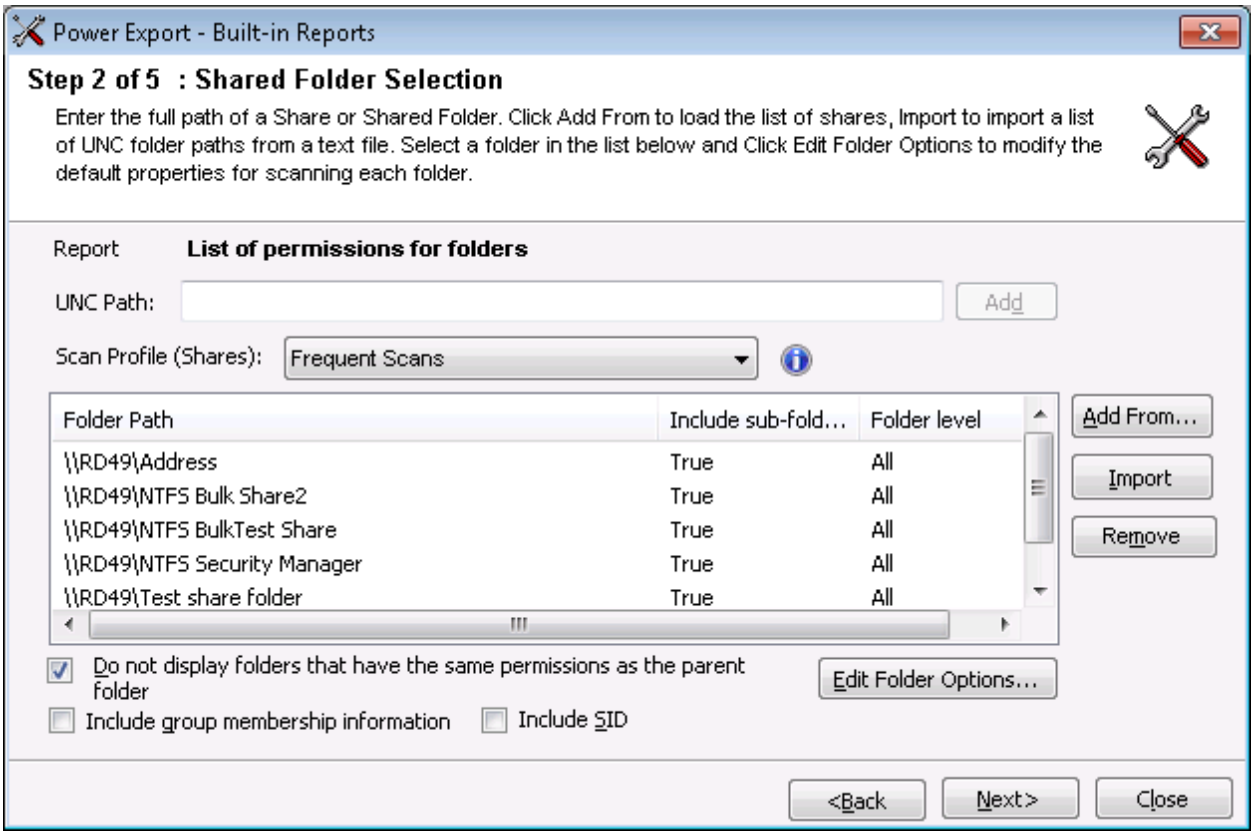
button in the toolbar.

Select any one of the permissions reports listed above and click Next to proceed.

In the next step, select the option 'Select a Scan Profiles (Shares)' as shown below.

Power Export - Built-in Reports
Step 2 of 5 : Shared Folder Selection
Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.
Report
List of permissions for folders
UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Include sub-fold...
Folder level
Add From...
Import
Remove
Do not display folders that have the same permissions as the parent folder
Edit Folder Options...
Include group membership information
Include SID
<Back
Next>
Close

- In this step the list of shares present in Scan Profile (Shares) will be loaded to the selected account list as shown below.



- In the succeeding steps select needed details for generating reports for selected shares.

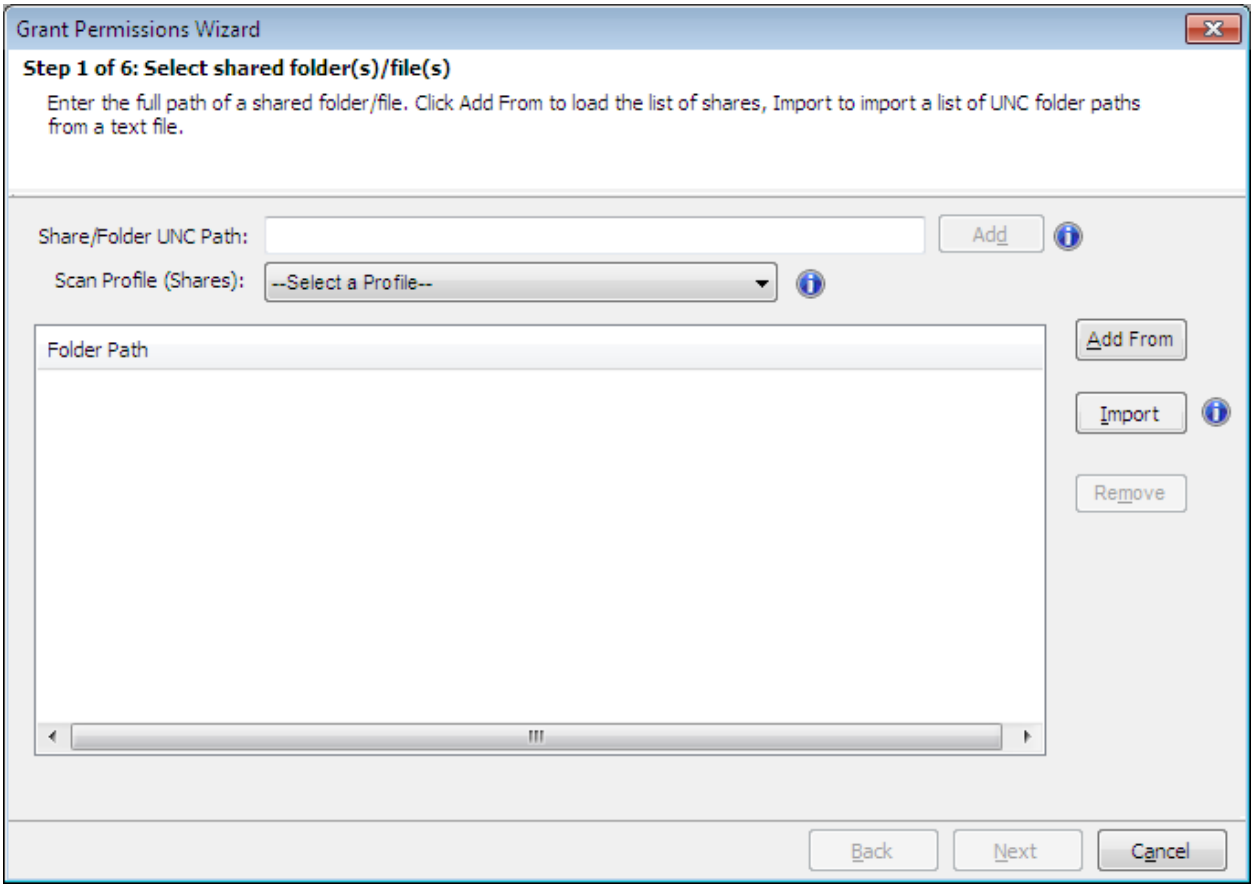
How to apply Scan Profiles (Shares) in NTFS Security Manager Module?

You can apply Scan Profile (Shares) to Grant Permissions, Revoke Permissions, Copy Permissions and also Modify Permissions that involves changes to permissions for the accounts on shared folder(s)/file(s). The following steps describe on how to apply Scan Profiles (Shares) in the Grant Permissions wizard.

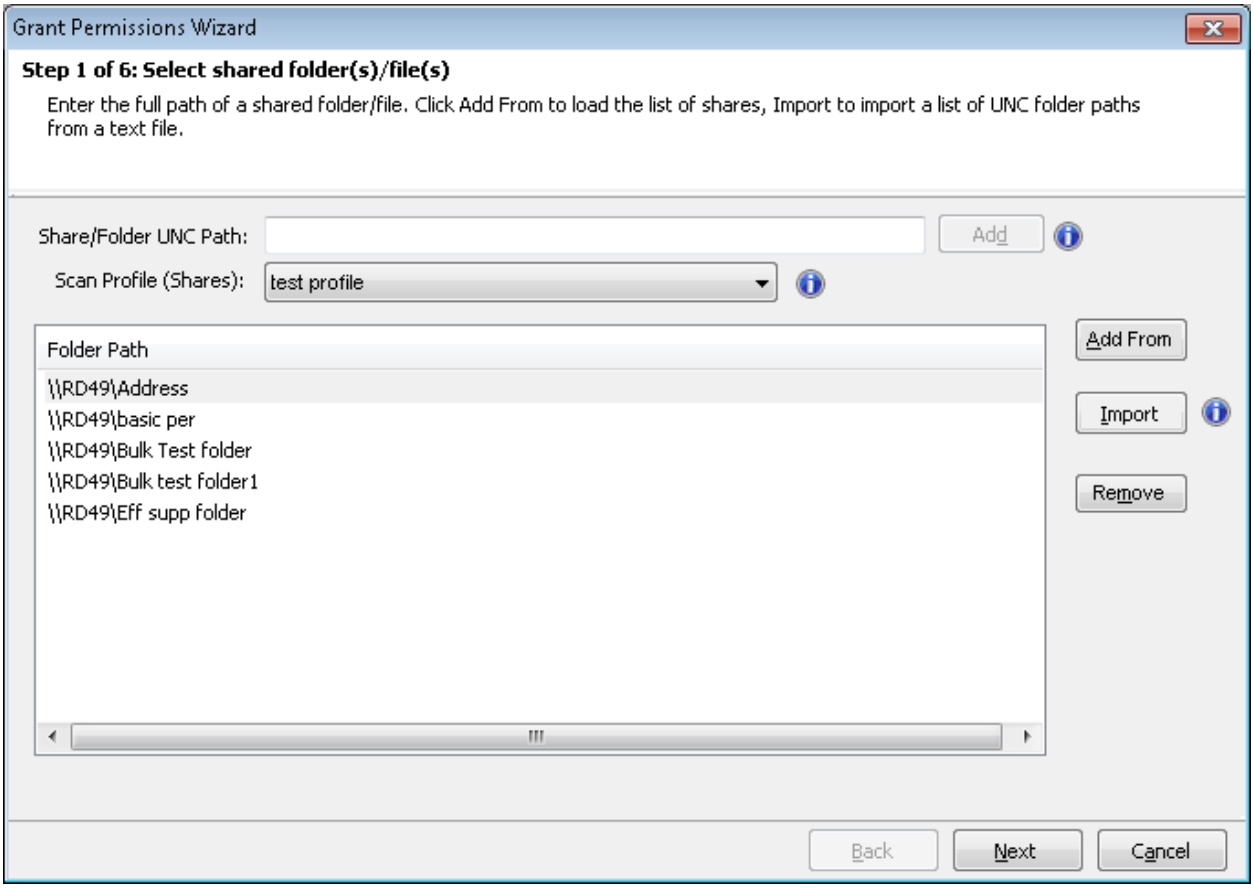
Click on

button in the toolbar.

The Grant Permissions window will be displayed as shown below:


Grant Permissions Wizard
Step 1 of 6: Select shared folder(s)/file(s)
Enter the full path of a shared folder/file. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.
Share/Folder UNC Path:
Add
Scan Profile (Shares):
--Select a Profile--
Folder Path
Add From
Import
Remove
Back
Next
Cancel

- Select a profile from the Scan Profile (Shares) dropdown to use the shares added in a profile.
- The list of shared folder(s)/file(s) present in the selected Scan Profile (Shares) will be loaded to the wizard as shown below.



- In the subsequent steps, select the necessary details for granting permissions for the shared folder(s)/file(s) present in the Scan Profile (Shares).

References

Frequently Asked Questions

Troubleshooting

How to uninstall NTFS Security Management Suite 2014

Frequently Asked Questions

For frequently asked questions about the product, please refer to the page **Frequently Asked Questions** in the website of the respective modules.

NTFS Security Auditor – FAQ

NTFS Security Manager – FAQ

NTFS Change Auditor – FAQ

Troubleshooting

If and when a problem arises, please forward the following information to support@vyapin.com to revert back to you with a solution. These files will be available where NTFS Security Management Suite 2014 is installed.

Error Log File

E.g., <Application Data>\NTFS Security Management Suite 2014\NTFSSecurityManagementSuite2014ErrorLog.Log

Note:

< Application Data> is the common area where NTFS Security Management Suite 2014 settings will be stored in the machine running NTFS Security Management Suite 2014.The <Application Data Folder> can be found from the Help -> About screen. The default path of <Application Data Folder> is as follows:

a) Windows XP, Windows 2003 - C:\Documents and Settings\All Users\Documents

b) Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Vista, Windows 7, Windows 8, Windows 8.1 - C:\Users\Public\Documents

How to uninstall NTFS Security Management Suite 2014?

When you uninstall NTFS Security Management Suite 2014 through Control Panel - Add / Remove Programs applet, Windows Installer program will remove only the application files from your machine. But, the application related files created by NTFS Security Management Suite 2014 remain in the computer. In order to remove NTFS Security Management Suite 2014 worker files completely, the uninstall wizard provides a set of cleanup options to perform the cleanup operation based upon your selection.

Use this wizard to cleanup the files that are created by NTFS Security Management Suite 2014 application selectively and uninstall NTFS Security Management Suite 2014 completely from the machine.

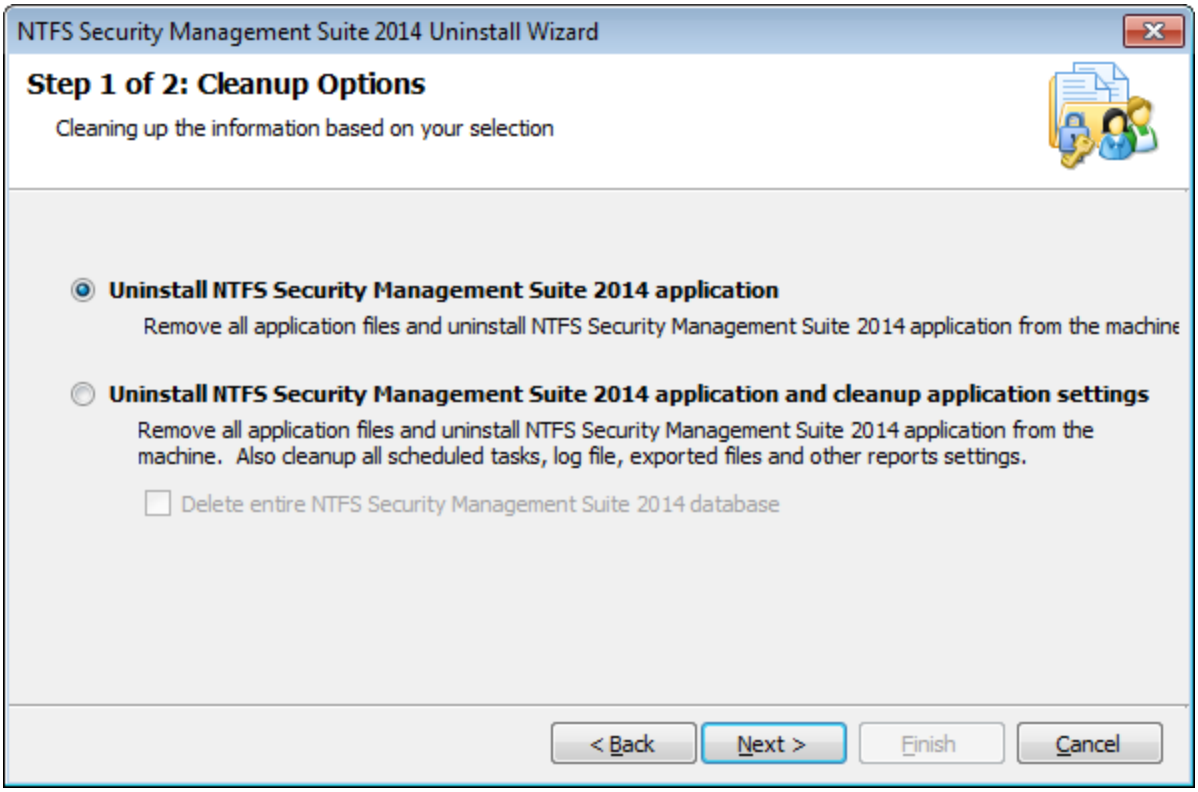
1.Launch the uninstall wizard by clicking Start -> Programs -> NTFS Security Management Suite 2014 -> NTFS Security Management Suite 2014 Uninstall Wizard.

The **NTFS Security Management Suite 2014 Uninstall Wizard** dialog will be shown as below:

NTFS Security Management Suite 2014 Uninstall Wizard
Welcome to NTFS Security Management Suite 2014 Uninstall Wizard
This wizard helps you to cleanup and uninstall NTFS Security Management Suite 2014 completely.
This wizard will guide you through the steps to cleanup the files that are created by NTFS Security Management Suite 2014 application.
Using this wizard you can:
* Cleanup scheduled tasks.
* Cleanup NTFS Security Management Suite 2014 application settings
* Cleanup log files
* Cleanup Scan Profiles created by NTFS Security Management Suite 2014 Scan Profile Manager
* Uninstall NTFS Security Management Suite 2014 application
< Back
Next >
Finish
Cancel

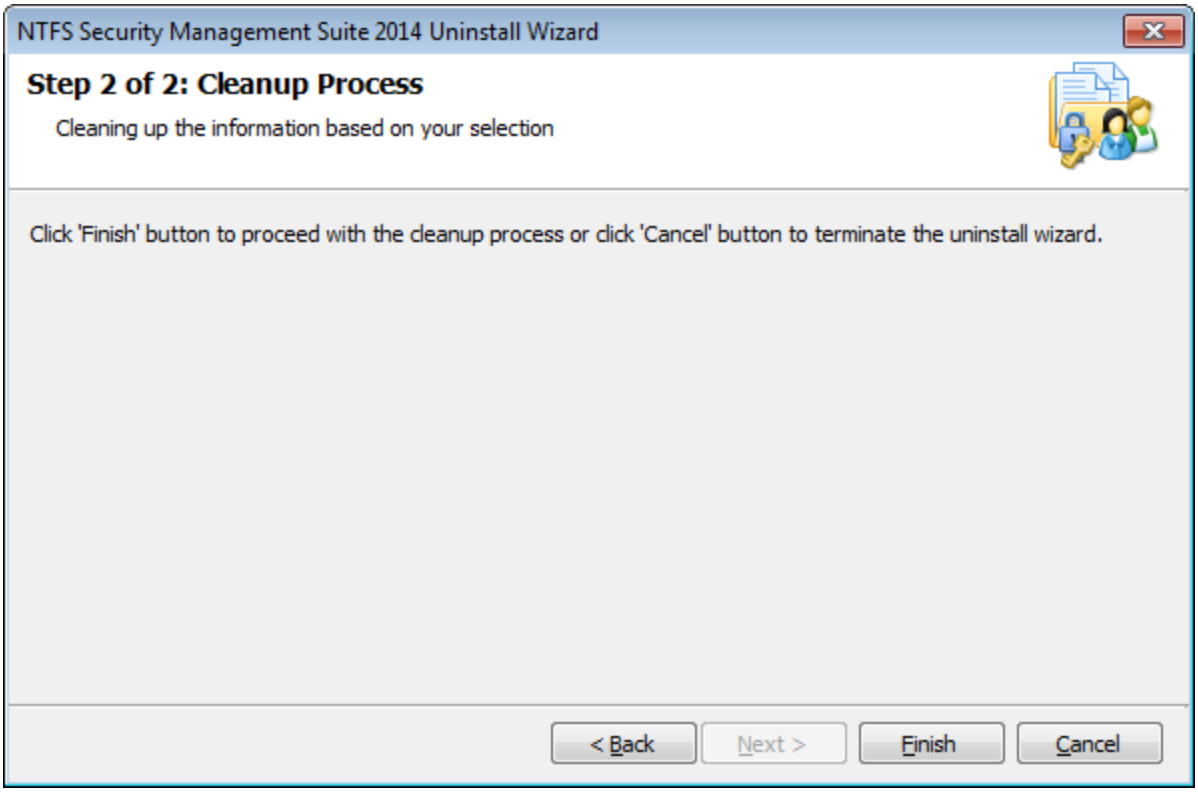
Click **Next** to proceed.

2. Select required cleanup options as shown below:


NTFS Security Management Suite 2014 Uninstall Wizard
Step 1 of 2: Cleanup Options
Cleaning up the information based on your selection
Uninstall NTFS Security Management Suite 2014 application
Remove all application files and uninstall NTFS Security Management Suite 2014 application from the machine
Uninstall NTFS Security Management Suite 2014 application and cleanup application settings
Remove all application files and uninstall NTFS Security Management Suite 2014 application from the machine. Also cleanup all scheduled tasks, log file, exported files and other reports settings.
Delete entire NTFS Security Management Suite 2014 database
< Back
Next >
Finish
Cancel

Click **Next** to proceed.

3. Confirm the cleanup and/or uninstall process.


NTFS Security Management Suite 2014 Uninstall Wizard
Step 2 of 2: Cleanup Process
Cleaning up the information based on your selection
Click 'Finish' button to proceed with the cleanup process or click 'Cancel' button to terminate the uninstall wizard.
< Back
Next >
Finish
Cancel

Click **Finish** to run cleanup and/or uninstall process. Click **Cancel** to close the wizard.

4. Once the file cleanup process is complete, the uninstall wizard will automatically run Windows Installer program to remove NTFS Security Management Suite 2014 application from the machine.